DESARROLLO DE UN PROCEDIMIENTO PARA LA CAPTURA Y GESTIÓN DE EVIDENCIA FORENSE EN LAS ÁREAS DE ADMINISTRACIÓN Y DESARROLLO DE SOFTWARE DE LA EMPRESA PTESA

GUILLERMO ALFREDO ALVAREZ GUERRERO

UNIVERSIDAD PILOTO DE COLOMBIA
FACULTAD DE INGENIERIA
ESPECIALIZACION EN SEGURIDAD INFORMATICA
BOGOTÁ D.C.
2015

DESARROLLO DE UN PROCEDIMIENTO PARA LA CAPTURA Y GESTIÓN DE EVIDENCIA FORENSE EN LAS ÁREAS DE ADMINISTRACIÓN Y DESARROLLO DE SOFTWARE DE LA EMPRESA PTESA

GUILLERMO ALFREDO ÁLVAREZ GUERRERO

Trabajo de grado

Asesor
John Jairo Echeverry Aristizabal
Master en Auditoría, Seguridad, Gobierno y Derecho de las TIC`s

UNIVERSIDAD PILOTO DE COLOMBIA
FACULTAD DE INGENIERIA
ESPECIALIZACION EN SEGURIDAD INFORMATICA
BOGOTÁ D.C.
2015

CONTENIDO

pág.

LISTA DE TABLAS

pág.

LISTA DE FIGURAS

pág.

LISTA DE ANEXOS

pág.

GLOSARIO

ATAQUES INFORMÁTICOS. Método premeditado y organizado que es ejecutado mediante un sistema informático con el propósito de tomar control, desestabilizar o dañar otro sistema informático.

AUTENTICIDAD. Propiedad de la información por la cual se garantiza su origen de tal modo que es posible demostrar que su emisor es quien dice ser.

BIT. Mínima unidad de medida utilizada en informática para representar 1 o 0 significando encendido o apagado y que se utiliza para el guardado de datos en medios de almacenamiento digitales.

CADENA DE CUSTODIA. Procedimiento de control que se aplica a elementos de evidencia desde su recolección hasta el final de su vida útil y que tiene como fin evitar alteraciones o cualquier contaminación o destrucción.

CIBERSEGURIDAD. Conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de una organización y los usuarios en el ciberentorno.

CONFIDENCIALIDAD. Servicio de seguridad que garantiza que la información sólo es accesible de forma legible para personas autorizadas.

CONPES. Siglas de Consejo Nacional de Política Económica y Social. Es la máxima autoridad nacional de planeación y se desempeña como organismo asesor del Gobierno en todos los aspectos relacionados con el desarrollo económico y social del país[1].

DATOS VOLÁTILES. Datos que pueden contener evidencia forense que están almacenados en los medios de memoria volátil de un equipo de cómputo tal como la memoria RAM los cuales se pierden en el momento de interrumpirse el flujo eléctrico.

DISCO DURO. Término informático que hace referencia a dispositivos de almacenamiento de datos digitales de alta capacidad que pueden ser internos cuando están insertados de forma permanente en un computador o externos cuando pueden ser conectados o extraídos de un computador de acuerdo con la necesidad.

[1] COLOMBIA. DEPARTAMENTO NACIONAL DE PLANEACIÒN. El Consejo Nacional de Política Económica y Social, CONPES [online]. Portal Web DNP. Actualizado 29 de mayo de 2015. Disponible en < https://www.dnp.gov.co/CONPES/Paginas/conpes.aspx>.

DISPONIBILIDAD. Servicio de seguridad que garantiza que la información es accesible de forma legible para personas autorizadas siempre que es requerida.

ESTERILIZACIÓN. Aplicado a medios digitales, es el proceso de eliminación segura de la información existente previamente en un medio de almacenamiento digital, es decir, sin que queden rastros de información que haya sido almacenada previamente en el medio.

EVIDENCIA FORENSE. Todo indicio que permite establecer a través de métodos científicos, una relación entre un crimen y quien lo cometió.

FORENSIA. Término relativo a técnicas y actividades forenses.

IMAGEN FORENSE. Copia bit a bit de un medio de almacenamiento digital en la cual quedan grabados los datos tal y como se encuentran en el medio original.

INFORMÁTICA FORENSE. Ciencia de adquirir, preservar, recuperar y presentar los datos que han sido procesados electrónicamente y almacenados en soportes informáticos[2] en relación con la investigación de un delito.

IMPACTO. Medida de las consecuencias que puede generar la materialización de una amenaza de seguridad.

INCIDENTE DE SEGURIDAD INFORMÁTICA. Cualquier hecho que afecta o podría afectar la seguridad informática de la organización.

INTEGRIDAD. Servicio de seguridad que garantiza que la información es creada o modificada sólo por personas autorizadas.

INTRUSIÓN. Acceso no autorizado a un sistema informático.

ISO. Siglas en inglés de Organización Internacional de Estandarización (International Standarization Organization), entidad internacional que a través de comités establecidos en varios países, emite normas de estandarización.

MALWARE. Término informático que se refiere a todo elemento de software malintencionado elaborado con el fin de infiltrarse, dañar o modificar sistemas de información sin el consentimiento del propietario.

[2] NOBLETT, Michael; POLLITT, Mark y PRESLEY, Lawrence. Recovering and Examining Computer Forensic Evidence [online]. Forensics Science Communications. Volume 2. Number 4. Octubre 2000. Disponible en <http://www.fbi.gov/about-us/lab/forensic-science-communications/fsc/oct2000/computer.htm/>

MEDIOS DE ALMACENAMIENTO. Medios físicos donde es posible almacenar los datos de sistemas computarizados y posteriormente leerlos o recuperarlos.

NORMAS ISO. Conjunto de estándares, modelos o criterios desarrollados por la Organización Internacional de Estandarización (ISO) que normalizan procesos de diversas índoles.

PTESA. Acrónimo de Profesionales en Transacciones Electrónicas. Nombre de la empresa tomada como base para la realización del trabajo de grado.

RAM: Sigla de Random Access Memory o memoria de acceso aleatorio que es el espacio de almacenamiento de datos temporal de una computadora y donde se alojan los datos que permiten operaciones de lectura y escritura.

SEGURIDAD DE LA INFORMACIÓN. Conjunto de normas preventivas y reactivas que se toman frente a los sistemas de información de una organización con el fin de resguardar y proteger las características de la información: integridad, confidencialidad y disponibilidad.

SOFTWARE. Término que se usa en informática para referirse a un conjunto de sentencias o rutinas que indican a un computador qué hacer.

VULNERABILIDAD. Debilidad de un sistema informático que puede ser aprovechada por una amenaza para causar daños o alteraciones en el sistema.

RESUMEN

En el presente trabajo se realiza un compendio normativo a partir de la legislación colombiana y de normas y estándares internacionales en relación con la seguridad informática, y particularmente en lo relativo a la conformación de grupos de gestión de incidentes de seguridad informática, identificación, recolección y gestión de evidencia forense de naturaleza digital y procedimientos de cadena de custodia. A partir de dicho compendio se plantea la conformación de un grupo de respuesta a incidentes de seguridad informática en la empresa PTESA, sus características, funciones y composición, así como la elaboración de un procedimiento de captura y gestión de evidencia forense en las áreas administrativas y de desarrollo de software de la misma empresa. Este procedimiento incluye instructivos detallados y formatos que se constituyen como material de orientación y apoyo para el funcionamiento del grupo de respuesta a incidentes. Informática forense, evidencia, cadena de custodia, bitácora, procedimiento.

INTRODUCCIÓN

Implementar sistemas de gestión de calidad y metodologías para la optimización de procesos es un estandarte en aquellas organizaciones competitivas de alto desempeño que buscan la productividad y el rendimiento.

Para ello se ha tornado fundamental la evaluación de las metodologías utilizadas dentro de sus actividades diarias, así como las tecnologías disponibles en pro de desarrollar sistemas que generen valor a través de la garantía, utilidad y eficacia de la gestión de información.

Con base en lo anterior, se hace énfasis en el diseño, implementación, operación y mejora continua de servicios tecnológicos que brindan grandes beneficios para potenciar las capacidades y logros de una corporación, reduciendo gastos mientras se aumenta la competitividad.

Una plataforma y servicios eficaces interconectados entre sí, ofrecen un abanico de oportunidades para el acceso y manejo de la información de cada empresa en el momento y condiciones que se establezcan en la implementación. Para ello se debe tener en cuenta un factor fundamental como lo es la seguridad de todos los datos administrados, garantizando su autenticidad, confidencialidad, integridad y disponibilidad con el fin de incrementar la percepción positiva de sus clientes haciéndoles saber que se llevan a cabo todas las medidas posibles para que su confianza no sea defraudada.

La seguridad es un término con el que cualquier ser humano puede identificarse, pues se trata de una necesidad humana elemental. De acuerdo con la teoría de Maslow, las necesidades humanas se pueden representar en una pirámide en cuya base están aquellas que son esenciales para la supervivencia, tales como la alimentación, el descanso o la respiración. Una vez satisfechas esas necesidades, en el segundo nivel está la seguridad, que se puede definir como una sensación de confianza o como la ausencia de peligro. Siendo esta una necesidad tan sentida para el hombre a nivel individual, no es de extrañar que lo sea también para cuando se conforman agrupaciones humanas en la sociedad, como es el caso de las empresas. En estas organizaciones, la seguridad se aborda desde diversas perspectivas una de las cuales tiene que ver con uno de los activos más valiosos de ellas: la información.

En los últimos años, las vulneraciones de la seguridad de la información en las empresas se han incrementado notablemente, provocando pérdidas millonarias por concepto de robo de información, fraudes y otros delitos conexos. Ante esta realidad se han realizado esfuerzos significativos tendientes a minimizar los riesgos de intrusiones, implementando diversos mecanismos tanto preventivos como reactivos en las organizaciones. Sin embargo, de acuerdo con una publicación realizada por la Corporación Colombia Digital, pese a que el 82% de las empresas latinoamericanas tienen un departamento encargado de monitorear los ataques informáticos, el 41% ha sufrido una infección por malware[3], información que deja entrever que la probabilidad de materializarse algún tipo de intrusión, aún en presencia de mecanismos de control, es bastante alta.

Con el fin de determinar las causas y los responsables de las intrusiones de seguridad que se presentan, se han venido desarrollado desde tiempo atrás, técnicas de informática forense que pueden ser aplicadas en escenarios en los que los atacantes de los sistemas informáticos logran tener éxito, permitiendo recolectar y procesar de manera adecuada la evidencia generada durante el ataque. Así, no solo se pone a disposición de las empresas herramientas suficientes para reaccionar ante estos eventos indeseados, sino también proponer alternativas de solución para evitar futuras intrusiones.

Por tanto, a través de este trabajo se pretende elaborar un procedimiento para la captura y gestión de evidencia forense en las áreas de administración y de desarrollo de software de la empresa PTESA, que permita recolectar y preservar evidencia para su utilización, en caso de que se materialice una amenaza de seguridad informática, para la detección de las vulnerabilidades explotadas, la aplicación de controles que sean pertinentes para evitar reincidencias y también asegurar que dicha evidencia pueda ser utilizada en un eventual proceso judicial.

[3] Corporación Colombia Digital. Perspectiva de la Seguridad Informática en Latinoamérica. Colombia Digital [online]. Julio 2, 2014. Disponible en <http://colombiadigital.net/actualidad/noticias/item/7289-perspectiva-de-la-seguridad-informatica-en-l atinoamerica.html>

1. JUSTIFICACIÓN

Los sistemas computarizados almacenan y procesan grandes volúmenes de información sensible de diferente índole, en consecuencia es posible que se generen escenarios que permitan la explotación de vulnerabilidades al interior de las organizaciones, esto debido al aumento de los ataques informáticos, los cuales son más sofisticados a medida que pasa el tiempo, y a la falta de controles de seguridad que permitan asegurar las características de los datos –integridad, confidencialidad y disponibilidad-.

Para las organizaciones, Identificar las causas y los responsables de los ataques informáticos es de vital importancia pues de esta manera se pueden determinar los medios y métodos utilizados para vulnerar la seguridad, y así aplicar los correctivos que sean necesarios para evitar que las mismas vulnerabilidades vuelvan a ser explotadas.

Una vez se determina que se presentó una vulneración de seguridad, es importante identificar con claridad los indicios de la misma, es decir, cualquier huella digital generada en los sistemas afectados durante el ataque; esto es lo que se conoce en informática forense, la cual consiste en la administración de evidencia digital. Debido a la fragilidad de este tipo de evidencia, se requiere aplicar métodos de recolección y administración adecuados con el fin de no contaminarla o inutilizarla y así poder usarla en procesos de análisis de seguridad e incluso, de ser necesario, llevarla ante instancias judiciales. No tener en cuenta esto expone a las organizaciones a ser blancos de ataques que pueden terminar en pérdidas significativas tanto de tipo económico como de reputación.

Desde el punto de vista de cumplimiento de la legislación colombiana y frente a lo establecido en la Ley 1273 de 2009, los datos almacenados en los sistemas informáticos se convierten en bienes jurídicos tutelados. También según lo establecido en Ley 1581 de 2012, las empresas deben asegurar que los datos personales de los ciudadanos estén protegidos y que sean administrados adecuadamente; no tomar las medidas pertinentes para el cumplimiento de estas disposiciones, expone a las compañías a recibir sanciones de alto impacto que puede llevarlas incluso a su culminación.

Frente a este escenario, en caso de presentarse una vulneración de la seguridad, es conveniente prever la manera de capturar la información suficiente y necesaria para plantear e implementar alternativas de solución, identificar al agresor, determinar responsabilidades y eventualmente iniciar procesos judiciales o

disciplinarios sustentados. Siendo la informática forense la aplicación de técnicas científicas y analíticas especializadas que permiten identificar, preservar, analizar y presentar datos digitales que sean válidos como pruebas dentro de un proceso legal o disciplinario, se hace necesario observar esta disciplina con el fin de dar solución a esta problemática.

Por otra parte, las compañías se desenvuelven en un ambiente de alta competencia dado que muchas de ellas ofrecen los mismos bienes y servicios a los consumidores, procurando diferenciarse de sus contendientes a través de la calidad de los productos y servicios que producen y generando confianza en el consumidor. Con el fin de captar más y mejores clientes, las empresas procuran mantenerse a la vanguardia, lo que implica un permanente mejoramiento, elevado nivel de calidad y una adecuada gestión de los recursos disponibles. Este aspecto es particularmente relevante para las compañías que, como PTESA, ofrecen servicios tecnológicos, campo que se caracteriza por estar en continuo cambio y renovación. Para cubrir esta necesidad, actualmente existen marcos de gestión de calidad de sistemas informáticos tales como COBIT e ITIL los cuales buscan estandarizar y optimizar las operaciones relacionadas con las tecnologías de la información, definiendo y recopilando las mejores prácticas probadas y aceptadas mundialmente en el ramo. Estos marcos incluyen elementos de seguridad de la información como los definidos por estándares tales como el grupo de normas ISO 27000. La aplicación de los procedimientos planteados en el presente documento, permitirá a PTESA estar a tono con elementos de las normas y buenas prácticas establecidas en algunas de las normas ya mencionadas, particularmente frente a temas de administración de incidentes (ISO 27001) y en el manejo de la evidencia digital (ISO 27037).

En el caso particular de PTESA, hasta el momento no se han definido mecanismos para la captura y gestión de evidencia forense bajo una metodología y actividades que se ajusten a las mejores prácticas de la industria, de manera que la gestión de incidentes se afronta a partir del conocimiento empírico. La ausencia de una estandarización incide sobre la homogeneidad en el conocimiento común del departamento técnico sobre cómo recolectar y administrar la evidencia forense, impactando la calidad y eficiencia de los procesos existentes, los cuales actualmente están relacionados con tareas de soporte.

Es por ello que se decide llevar a cabo este proyecto, que consiste en la elección de una metodología que permitirá establecer las consideraciones necesarias para la captura y manejo de evidencia forense en la empresa PTESA, de manera particular en el área administrativa y en el área de desarrollo de software, con el propósito de dar validez a la información manejada, teniendo en cuenta las regulaciones legales y las recomendaciones de la industria.

2. PLANTEAMIENTO DEL PROBLEMA

Hasta el momento la información almacenada por PTESA se ha manejado con el mayor cuidado y aplicando controles de seguridad tendientes a evitar filtraciones de información sensible. A partir de los controles implementados, no se han detectado ataques informáticos que hayan implicado fuga o alteración de la información sensible administrada por la compañía, razón por la que no se ha visto la necesidad de definir mecanismos de captura y preservación de evidencia digital.

Sin embargo, dada la tendencia mundial de aumento de incidentes de seguridad y el crecimiento en la sofisticación de los métodos utilizados por los atacantes, es necesario mejorar los mecanismos de reacción ante eventuales vulneraciones de la seguridad, como es el caso del tema desarrollado en el presente trabajo en relación con los procedimientos de recolección y administración la evidencia digital. También frente a la regulación normativa colombiana y con miras a implementar las mejores prácticas de la industria, se identifica un punto de mejora importante en los procesos de aseguramiento de la información de la empresa PTESA.

De manera proactiva, surge la necesidad de plantearse una pregunta fundamental que va de la mano con la buena ejecución de la actividad principal de la compañía:

¿PTESA cuenta con procedimientos claramente definidos, documentados y adecuados para la captura y gestión de evidencia forense en sus sistemas computarizados en caso de que se presente una vulneración de la seguridad informática?

3. OBJETIVO GENERAL

Elaborar, diseñar y documentar un procedimiento para la captura y gestión de evidencia forense en los sistemas computacionales de las áreas administrativa y de desarrollo de software de la empresa PTESA.

3.1 OBJETIVO ESPECÍFICO

Socializar el procedimiento elaborado con el personal de la empresa PTESA.

4. MARCO TEÓRICO

4.1 MARCO LEGAL

A continuación se presenta una matriz que incluye el ordenamiento legal colombiano en relación con la seguridad de la información, la identificación de activos jurídicamente tutelados, la conformación de grupos de respuesta a incidentes de seguridad de la información y mecanismos legales que orientan la aplicación de las normas.

Tabla 1. Extracto de la Ley 527 de 1999

Documento	Descripción
Ley 527 de 1999	Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones. En el artículo 2 se introducen al sistema normativo algunas definiciones que tienen relevancia para el accionar forense como son: a) Mensaje de datos. b) Comercio electrónico. c) Firma digital. d) Entidad de Certificación. e) Intercambio Electrónico de Datos (EDI). f) Sistema de Información. Otros aspectos de importancia son: Artículo 3. Interpretación de la ley en concordancia con las normas internacionales. Artículo 5. Reconocimiento jurídico de los mensajes de datos. Artículo 6. Definición de medio escrito para todo mensaje de datos que pueda ser consultado posteriormente. Artículo 8. Definición de originalidad. Artículo 9. Integridad de un mensaje de datos. Artículos 10 al 13. Tocan aspectos relacionados con la admisibilidad de los mensajes de datos en estrados judiciales como pruebas. Si bien la ley tiene un enfoque primariamente comercial, contiene criterios de sumo valor para la labor forense.

Fuente: CONGRESO DE COLOMBIA. Ley 527 (18, agosto, 1999). Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones [online]. Bogotá D.C.: El Ministerio, 1999. Disponible en <http://www.archivogeneral.gov.co/sites/all/themes/nevia/PDF/Transparencia/LEY_527_DE_1999.pdf>

Tabla 2. Extracto de la Ley 599 de 2000

Documento	Descripción
Ley 599 de 2000	Artículo 293. Destrucción, supresión y ocultamiento de documento privado. El que destruya, suprima u oculte, total o parcialmente un documento privado que pueda servir de prueba, incurrirá en prisión de uno (1) a seis (6) años.

Fuente: CONGRESO DE COLOMBIA. Ley 599 (24, julio, 2000). Por la cual se expide el Código Penal [online]. Bogotá D.C.: El Ministerio, 2000. Disponible en < http://www.archivogeneral.gov.co/sites/all/themes/nevia/PDF/Transparencia/Codigo_Penal.pdf>

Tabla 3. Extracto de la Ley 1273 de 2009

Documento	Descripción
Ley 1273 de 2009	Por medio de la cual se crea un nuevo bien jurídico tutelado denominado "de la protección de la información y de los datos" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. Esta ley trata de los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos, tipificando delitos como los mencionados en los artículos: Artículo 269A: Acceso abusivo a un sistema informático Artículo 269B: Obstaculización ilegítima de sistema informático o red de telecomunicación Artículo 269C: Interceptación de datos informáticos Artículo 269D: Daño Informático Artículo 269E: Uso de software malicioso Artículo 269F: Violación de datos personales Artículo 269G: Suplantación de sitios web para capturar datos personales Se establecen además las sanciones a que dan lugar tales acciones, los agravantes punitivos y la asignación de jueces.

Fuente: CONGRESO DE COLOMBIA. Ley 1273 (5, enero, 2009). Por medio de la cual se modifica el código penal, se crea un nuevo bien jurídico tutelado denominado “de la protección de la información y de los datos” y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones [online]. Bogotá D.C.: El Ministerio, 2009. Disponible en <http://www.mintic.gov.co/portal/604/articles-3705_documento.pdf>

Tabla 4. Extracto de la Ley 1581 de 2012

Documento	Descripción
Ley 1581 de 2012	Por la cual se dictan disposiciones generales para la protección de datos personales. Los principios y disposiciones contenidas en esta ley son aplicables a los datos personales registrados en cualquier base de datos que los haga susceptibles de tratamiento por entidades de naturaleza pública o privada con excepción de los casos establecidos en la misma. Se establecen los derechos de los titulares de la información y los deberes de los entes que la administran o procesan, así como las sanciones a que da lugar el incumplimiento de las disposiciones establecidas.

Fuente: COLOMBIA. PRESIDENTE DE LA REPÚBLICA. Ley 1581 (17, octubre, 2012). Por la cual se dictan disposiciones generales para la protección de datos personales [online]. Diario Oficial. Bogotá, D. C., 2012. Disponible en <http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=49981>

Tabla 5. Extracto del documento Conpes 3701

Documento	Descripción
Conpes 3701	Mediante el cual se "busca generar lineamientos de política en ciberseguridad y ciberdefensa orientados a desarrollar una estrategia nacional que contrarreste el incremento de las amenazas informáticas que afectan significativamente al país".

Fuente: COLOMBIA. CONSEJO NACIONAL DE POLÍTICA ECONÓMICA Y SOCIAL. LINEAMIENTOS DE POLÍTICA PARA CIBERSEGURIDAD Y CIBERDEFENSA [online]. Bogotá D.C. (14, julio, 2011). Disponible en <http://www.mintic.gov.co/portal/604/articles-3510_documento.pdf>

Tabla 6. Extracto de la Decreto 1377 de 2013

Documento	Descripción
Decreto 1377 de 2013	Decreto que reglamenta parcialmente la Ley 1581 de 2012 y que busca facilitar la implementación y el cumplimiento de la misma, particularmente en "aspectos relacionados con la autorización del Titular de información para el Tratamiento de sus datos personales, las políticas de Tratamiento de los Responsables y Encargados, el ejercicio de los derechos de los Titulares de información, las transferencias de datos personales y la responsabilidad demostrada frente al Tratamiento de datos personales".

Fuente: COLOMBIA. PRESIDENTE DE LA REPÚBLICA. Decreto 1377 (27, junio, 2013). Por el cual se reglamenta parcialmente la Ley 1581 de 2012 [online]. Diario Oficial. Bogotá, D. C., 2013. No. 48834 Disponible en <http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=53646>

Tabla 7. Extracto de la Ley 1712 de 2014.

Documento	Descripción
Ley 1712 de 2014	Regula el derecho de acceso a información pública. Es importante dado que PTESA eventualmente puede almacenar información que se considera pública según lo determinado en la mencionada ley y además porque en ella se establecen elementos importantes para el manejo de la información siguiendo los estándares establecidos por el estado.

Fuente: COLOMBIA. CONGRESO DE LA REPUBLICA. Ley 1712 (6, marzo, 2014). Por medio de la cual se crea la ley de transparencia y del derecho de acceso a la información pública nacional y se dictan otras disposiciones [online]. Bogotá D.C.: El Ministerio, 2014. Disponible en <http://www.mintic.gov.co/portal/604/articles-7147_documento.pdf>

Tabla 8. Extracto de la Ley 906 de 2004.

Documento	Descripción
Ley 906 de 2004	Establece en su artículo 275, los mensajes de datos como elementos materiales probatorios y evidencia física con validez en procesos penales procesos penales.

Fuente: CONGRESO DE COLOMBIA. Ley 906 (1, septiembre, 2004). Por la cual se expide el Código de Procedimiento Penal. (Corregida de conformidad con el Decreto 2770 de 2004) [online]. Bogotá D.C.: El Ministerio, 2004. Disponible en <http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=14787>

4.2 FUNDAMENTACIÓN TEÓRICA

4.2.1 Introducción. En este apartado se presentan extractos de normas internacionales y manuales elaborados por expertos en seguridad de la información que se tuvieron en cuenta para la elaboración del procedimiento al que se refiere este documento. Se da un vistazo a la definición de la informática forense y a algunos de sus principios rectores, particularmente los relacionados con la forensia en evidencia digital. A continuación se consideran aspectos a tener en cuenta para la adecuada recolección de evidencia y elementos de cadena de custodia que permitan salvaguardarla. Finalmente se mencionan recomendaciones para la elaboración de procedimientos de seguridad informática.

4.2.2 Informática forense. En esta sección se toman conceptos de la informática forense, su definición y propósito y posteriormente enfatizando en la evidencia digital, sus características más sobresalientes y los mecanismos de gestión definidos, probados y avalados a nivel internacional con el fin de asegurar que la evidencia no pierda sus características y validez.

4.2.2.1 Definición. El FBI define la informática forense como la ciencia de adquirir, preservar, recuperar y presentar los datos que han sido procesados electrónicamente y almacenados en soportes informáticos[4]. Esta disciplina surgió de la necesidad de hacer aplicar la ley frente a pruebas existentes en formatos electrónicos y tiene un ámbito de acción diferente al de las otras disciplinas forenses puesto que es posible tratar la evidencia utilizando un computador prácticamente en cualquier ubicación y no solamente en laboratorios especializados. Los resultados obtenidos en esta disciplina también son diferentes de los proporcionados por otras disciplinas en la medida en que no proporcionan pruebas que dependen de la interpretación sino que analiza y produce datos de valor específico para una investigación.

La informática forense abarca varios aspectos como la computación forense, la forensia en redes y la forensia digital. Esta última se refiere al uso de métodos científicamente probados y orientados hacia la preservación, recolección, validación, identificación, análisis, interpretación, documentación y presentación de evidencia digital, derivada de fuentes digitales, con el propósito de facilitar o promover la reconstrucción de hechos o ayudando a anticipar acciones no autorizadas que hayan demostrado ser perjudiciales[5].

Para efectos alcanzar el objetivo del presente trabajo, se logró establecer que la informática forense es la disciplina más idónea para la elaboración de un procedimiento de recolección y gestión de evidencia forense pues proporciona las bases conceptuales y metodológicas más adecuadas para ello.

4.2.2.2 Evidencia forense. El conocimiento de la evidencia, sus características y utilidad en procesos de investigación de las causas de incidentes de seguridad, es de suma importancia para PTESA pues permitirá concienciar al personal sobre la necesidad de ubicar y administrar dicha evidencia adecuadamente, de tal forma que pueda ser de utilidad en el perfeccionamiento y afinamiento de los procesos internos de la empresa y eventualmente para su utilización en eventuales procesos disciplinarios o legales en caso de requerirse frente a la comisión de un delito.

[4] NOBLETT, Michael; POLLITT, Mark y PRESLEY, Lawrence. Recovering and Examining Computer Forensic Evidence [online]. Forensics Science Communications. Volume 2. Number 4. Octubre 2000. Disponible en <http://www.fbi.gov/about-us/lab/forensic-science-communications/fsc/oct2000/computer.htm/>

[5] THE FIRST DIGITAL FORENSIC RESEARCH WORKSHOP (DFRWS). A Road Map for Digital Forensic Research [online]. Technical Report. DTR - T001-01 FINAL. Utica, New York, August 7-8, 2001. November 6th, 2001 – Final. Disponible en <http://www.dfrws.org/2001/dfrws-rm-final.pdf>

De acuerdo con el diccionario de la real academia de la lengua española, la evidencia es una prueba que puede ser determinante en un proceso. En relación con las ciencias forenses, la evidencia son todos aquellos elementos que se encuentran en la escena de un crimen y que pueden permitir identificar a los responsables. Según el principio de Locard, “siempre que dos objetos entran en contacto, se transfieren elementos que incorporan al otro objeto”. Siendo así, a partir de los indicios o evidencias que se encuentran en la escena de un crimen, es posible determinar la relación de individuos con los hechos delictivos que se investigan, al establecer su presencia en el lugar y el momento de los hechos y su relación con ellos.

4.2.2.3 Evidencia digital. Para el Grupo de Trabajo sobre la Evidencia Digital (SWGDE), Organización Internacional de Evidencia Digital (IOCE), el término "evidencia" implica que el colector de la evidencia es reconocido por los tribunales. El proceso de recolección también se supone que es un proceso legal y apropiado para reglas de evidencia en una localidad. Un objeto de datos o elemento físico sólo se convierte en evidencia cuando así se considere por un oficial de la ley o la persona designada[6]. Esto implica que se debe prestar especial cuidado no solo a la información que se recolecta sino también a las personas que están involucradas en el proceso y al método utilizado.

En Colombia la importancia de los elementos mencionados anteriormente se dejó ver con total claridad en el caso de alias Raúl Reyes, miembro del secretariado de la guerrilla de las FARC abatido en marzo de 2008 y en cuyo poder se encontraron numerosos dispositivos electrónicos que contenían cuantiosa información de alto valor para los mandos militares, pero que no pudo ser utilizada en los estrados judiciales debido a que las personas que recolectaron los dispositivos no tenían jurisdicción para realizar el levantamiento de la información en el lugar donde esta fue encontrada, y también a que las acciones ejecutadas sobre dichos dispositivos no se ajustaron a las disposiciones técnicas requeridas para el manejo de evidencia digital, en concordancia con los estándares internacionales.

En PTESA, siendo una entidad privada sujeta a la normatividad colombiana, la aplicación de los principios ya expuestos acerca de la evidencia digital no pueden ser menos rigurosos; de allí la necesidad de asegurar que el personal que tenga relación con la evidencia digital, tenga pleno conocimiento tanto del ordenamiento

[6] THE FIRST DIGITAL FORENSIC RESEARCH WORKSHOP (DFRWS). INTERNATIONAL ORGANIZATION ON DIGITAL EVIDENCE (IOCE). Digital Evidence: Standards and Principles [online]. Volume 2. Number 2. Abril 2000. Disponible en <http://www.fbi.gov/about-us/lab/forensic-science-communications/fsc/april2000/swgde.htm/>

legal colombiano como de las mejores prácticas reconocidas a nivel internacional en relación con ella.

4.2.2.4 Características de la evidencia digital. Según lo establecido en la norma ISO 27037, para que la evidencia forense tenga valor probatorio, se debe asegurar el cumplimiento de los siguientes principios*:*

- Relevancia. Se debe poder determinar la importancia que tiene la evidencia en el proceso investigativo que se está llevando a cabo. Debe existir una justificación clara de la razón por la que los datos fueron obtenidos.

- Fiabilidad. Todos los procesos utilizados para la captura de la evidencia están auditados y son repetibles, es decir que es posible reproducir los resultados obtenidos aplicando los procesos ejecutados.

- Suficiencia. El material obtenido es suficiente para permitir llevar a cabo la investigación[7].

El personal de la empresa PTESA que forme parte del grupo de respuesta a incidentes y que por lo tanto tenga como responsabilidad la ejecución del procedimiento de captura de evidencia, deberá tener claros estos principios para poder identificar los elementos relevantes en un proceso de investigación forense y para que lleve a cabo las actividades requeridas por el procedimiento con la debida rigurosidad.

4.2.2.5 Manejo de evidencia digital. Una vez establecidas las características de la evidencia y asumiendo que existe la capacidad de identificarla, se hace necesario establecer los mecanismos más apropiados para su recolección y administración, tópicos que se abarcan a continuación, con el fin de evitar que la evidencia pierda sus características y por lo tanto su *utilidad.*

[7] INTERNATIONAL STANDARD ISO/IEC 27037. Information technology — Security techniques — Guidelines for identification, collection, acquisition, and preservation of digital evidence. Primera edición. 2012. Página 6.

Requerimientos

La norma ISO mencionada anteriormente indica que existen cuatro principios claves en el manejo de la evidencia digital, a saber:

- Auditabilidad. Un evaluador acreditado independiente o de alguna de las partes interesadas debe poder evaluar las acciones realizadas sobre la evidencia por lo cual se necesita que todas las actividades estén adecuadamente documentadas. El personal que haya tomado parte en las acciones ejecutadas sobre la evidencia debe estar en capacidad de justificar el proceso de toma de decisiones en la selección de un determinado curso de acción. Los procesos llevados a cabo deben estar disponibles para determinar de manera independiente si se siguió un adecuado método científico, técnica o procedimiento[8].

- Repetibilidad. Se produce cuando al realizar una prueba se producen los mismos resultados bajo las siguientes condiciones: se utiliza el mismo procedimiento y método de medición, se utilizan los mismos instrumentos bajo las mismas condiciones y el resultado puede ser reproducido en cualquier momento después de la prueba original. Un primer respondiente debidamente cualificado y con experiencia debe ser capaz de llevar a cabo todos los procesos descritos en la documentación y llegar a los mismos resultados, sin guía o interpretación. El primer respondiente debe ser consciente que puede haber circunstancias en las que no sería posible repetir la prueba, por ejemplo, cuando un disco duro original o unidad ha sido copiado y vuelto a usar, o cuando un elemento implica memoria volátil. En este caso, el primer respondiente debe asegurar que el proceso de adquisición es confiable. Para lograr la repetibilidad, el control de calidad y la documentación del proceso deben estar en su lugar[9].

- Reproducibilidad. Se establece cuando los mismos resultados de la prueba se producen bajo las siguientes condiciones: se utiliza el mismo método de medición, se usan diferentes instrumentos y diferentes condiciones y puede ser reproducido en cualquier momento después de la prueba original[10].

- Justificabilidad. El primer respondiente debe ser capaz de justificar todas las acciones y métodos utilizados en el manejo de la potencial evidencia digital. Se debe poder demostrar que la decisión tomada era la mejor opción para obtener

[8] Ibid., p. 7.
[9] Ibid., p. 7.
[10] Ibid., p. 7.

toda la evidencia digital potencial. Otro profesional también podría demostrar esto mediante la exitosa reproducción o la validación de las acciones y los métodos utilizados[11].

Alcance

En relación con los procedimientos de manejo de la evidencia digital, la norma ISO 27037 establece como alcance los pasos iniciales que son: identificación, recolección, adquisición y preservación de la evidencia digital potencial. En su estado natural la evidencia es muy frágil y puede ser alterada o dañada fácilmente si no se maneja o examina de manera apropiada; por tanto, los procedimientos establecidos para el manejo de la evidencia digital deben incluir los siguientes principios fundamentales:

- Manipular en lo mínimo el dispositivo que contiene la evidencia original.

- Reportar cualquier cambio y documentar las acciones realizadas

- Cumplir con la reglamentación local en relación con la evidencia digital y

- El personal que maneja la evidencia no debe tomar acciones más allá de su competencia[12].

A continuación se da un vistazo más profundo sobre los cuatro elementos mencionados en relación con los pasos iniciales de manejo de la evidencia.

- Identificación. La evidencia digital puede presentarse en forma física o lógica. Es evidencia física aquella contenida en un dispositivo tangible. La evidencia lógica se refiere a la representación virtual del contenido de un dispositivo. Este proceso también incluye una priorización de la adquisición de evidencia según su volatilidad. El orden en que se adquiera la evidencia puede afectar la calidad de la misma[13].

[11] Ibid., p. 7.
[12] Ibid., p. 8.
[13] Ibid., p. 8.

- Recolección. Una vez se ha determinado que un dispositivo puede contener evidencia potencial se deberá determinar si recolectarla o adquirirla. La decisión de tomar uno u otro camino depende de las circunstancias. La recolección consiste en transportar el dispositivo que contiene la evidencia digital potencial a un laboratorio donde posteriormente sea posible adquirir dicha evidencia en un ambiente controlado. Los dispositivos en mención pueden estar en dos estados: encendidos o apagados. Dependiendo del estado del dispositivo se utilizan unos u otros procedimientos y herramientas[14].

- Adquisición. El proceso de adquisición incluye producir copias de la evidencia y la documentación de los métodos y actividades ejecutadas. El personal involucrado utilizará un determinado método de adquisición dependiendo de la situación, el costo y el tiempo y deberá documentar apropiadamente la decisión de tomar un método o herramienta determinado. Los métodos deben estar también muy bien documentados así como cualquier alteración de los datos producto de la ejecución de las actividades durante el proceso. Las copias de la evidencia y las fuentes originales deben producir los mismos resultados al aplicarles funciones de verificación. En aquellas circunstancias donde no es posible ejecutar procesos de verificación, el personal que realiza la adquisición deberá documentar y justificar los métodos utilizados procurando que sean los más adecuados. En aquellos escenarios donde no es posible obtener copias completas de la evidencia se deberán extraer imágenes forenses de los datos relevantes siguiendo los mismos principios ya establecidos[15].

- Preservación. Es importante preservar la integridad de la evidencia potencial con el fin de que sea útil en la investigación evitando que sea alterada o manipulada. El proceso de preservación debe mantenerse durante todo el proceso de manejo de la evidencia comenzando desde la identificación de los dispositivos que contienen la evidencia potencial. El personal involucrado debe poder demostrar que la evidencia no fue modificada desde su adquisición o proveer las acciones documentadas de los cambios inevitables a que haya habido lugar durante el proceso[16].

A continuación se presentan algunos componentes claves de los 4 elementos considerados anteriormente.

[14] Ibid., p. 9.
[15] Ibid., p. 9.
[16] Ibid., p. 10.

4.2.4 Cadena de custodia. Los mecanismos de cadena de custodia buscan asegurar que los elementos de evidencia recolectados y gestionados durante un proceso de investigación forense no han sido adulterados, permitiendo hacer un seguimiento exhaustivo de cada uno de ellos desde su identificación hasta su disposición final. A continuación se presentan fundamentos teóricos y prácticos que fueron tenidos en cuenta para la elaboración del procedimiento de recolección y gestión de evidencia forense.

4.2.4.1 Consideraciones generales. De acuerdo con la Resolución 0-2869, "el Sistema de Cadena de Custodia debe asegurar las características originales de los elementos materia de prueba durante la protección de la escena, recolección, transporte, análisis, almacenamiento, conservación, preservación, recuperación y disponibilidad de éstos, identificando al responsable en cada una de sus etapas y que los elementos correspondan al caso investigado"[17]. Esta definición corresponde con la aplicación práctica de la normatividad colombiana en el tema en cuestión y por tanto arroja luz acerca de lo que se espera de la implementación de un sistema de cadena de custodia aceptable legalmente en el país.

4.2.4.2 Registro de la evidencia. En cualquier investigación de informática forense, el primer respondiente deberá estar en capacidad de registrar los datos y dispositivos adquiridos así como el momento en que estos entran en cadena de custodia. El registro de cadena de custodia es un documento que identifica cronológicamente los movimientos y el manejo que se da a la evidencia potencial incluyendo la traza histórica para cada elemento desde el momento en que fue identificado, recolectado o adquirido hasta el momento presente.

El propósito de tener registros de la cadena de custodia es permitir identificar los movimientos y el acceso a la evidencia potencial en cualquier punto de tiempo; el registro puede involucrar más de un documento y debe contener como mínimo lo siguiente:

- Un identificador único de evidencia.

- Quién tuvo acceso a la evidencia, el momento y el lugar en que esto sucedió.

[17] COLOMBIA. FISCALÍA GENERAL DE LA NACIÓN. Continuación de la Resolución 0-6394. (22, diciembre, 2004). Por medio de la cual se adopta el Manual de Procedimientos del sistema de cadena de custodia para el sistema penal acusatorio [online]. Página 19. Disponible en <http://www.usergioarboleda.edu.co/derecho_penal/pdf/2004-MANUAL CADENA DE CUSTODIA.pdf>

- Quién ingresó y extrajo la evidencia del repositorio establecido y cuándo sucedió.

- Por qué la evidencia fue extraída y la autoridad relevante si aplica.

- Cualquier cambio inevitable sobre la evidencia y el nombre del individuo responsable así como la justificación para la ocurrencia del cambio.

Los registros de cadena de custodia se deben mantener durante todo el ciclo de vida de la evidencia y un tiempo posterior a su vida útil de acuerdo con la legislación del lugar.

4.2.4.3 Administración de evidencia. En el Manual de Procedimientos del sistema de cadena de custodia establecido por la Fiscalía General de la Nación, se establecen los siguientes factores críticos de éxito a tener en cuenta en los procesos de administración de evidencia sin perder la trazabilidad de la cadena de custodia:

1. En la recolección de los elementos físicos de prueba:

- Utilice elementos de bioseguridad.

- Embale en bolsas o contenedores estériles, con el fin de asegurar y conservar las características de los elementos físicos de prueba.

2. En cada traspaso y traslado, el embalaje debe estar perfecto e íntegro, las bolsas no pueden presentar cortes.

3. El rótulo del elemento, no debe presentar tachones o enmendaduras y debe identificar plenamente el elemento. Éste documento no se debe retirar del embalaje.

4. El almacenamiento de los elementos físicos de prueba, debe ser en condiciones ambientales adecuadas para conservar las condiciones y características originales de los elementos físicos de prueba, contando con el espacio adecuado para que no se contaminen unos con otros.

5. El diligenciamiento del formato de cadena de custodia, se debe realizar de manera completa y organizada, sin presentar tachones o enmendaduras y debe identificar plenamente los traslados y traspasos, durante todo el proceso de cadena de custodia, en forma tal que se conozca la identidad de cada custodio y las acciones que realizó con el elemento.

6. Cumplir con las normas internas y externas que aplican sobre el tema.
Cada uno de los elementos mencionados anteriormente fueron tenidos en cuenta para la elaboración del instructivo de cadena de custodia donde se aplican y adaptan a las necesidades de la empresa PTESA.

4.2.4.4 Seguimiento de la evidencia. Mantener el control de todos los elementos que interactúan con la evidencia digital es un factor determinante a la hora de probar la imparcialidad y la confiabilidad de las personas que la han manipulado. Para poder demostrar que no se ha perdido el control de la evidencia, a través de los registros de cadena de custodia los investigadores deben estar en capacidad de responder a seis preguntas básicas[18]:

- ¿Quién controló la evidencia?
- ¿Qué se usó para recolectarla?
- ¿Por qué se hizo de esa manera?
- ¿Cuándo fue encontrada cada pieza de evidencia?
- ¿Dónde fue encontrada?
- ¿Cómo fue documentada?

[18] COBB, Chey. How to secure the chain of custody in a digital forensics investigation [online]. SearchITChannel. Diciembre 2007. Disponible en <http://searchitchannel.techtarget.com/tip/How-to-secure-the-chain-of-custody-in-a-digital-forensics-investigation>

4.2.5 Recolección de evidencia. Es necesario tener una metodología clara sobre la manera de recolectar la evidencia digital para no perder datos que sean relevantes, por tanto a continuación se presentan tres aspectos a tener en cuenta durante el proceso como son el aseguramiento del lugar del incidente, la adecuada selección del personal que lleve a cabo el procedimiento y las características de la documentación que se debe generar.

4.2.5.1 Precauciones en el lugar del incidente. Para preservar la escena del incidente se deben llevar a cabo las siguientes actividades:

- Asegurar y tomar control del lugar donde se encuentran los dispositivos.

- Determinar quién está a cargo del lugar.

- Asegurarse que las personas presentes se mantengan alejadas de los dispositivos y de las fuentes de alimentación de energía.

- Documentar cualquier persona que haya tenido acceso al lugar y las razones para estar involucradas con la escena del incidente.

- Si el dispositivo está encendido, no apagarlo; si está apagado, no encenderlo.

- En lo posible documentar la escena con todos sus componentes, incluyendo los cables en su posición original, preferiblemente usando cámara fotográfica o de video. En caso de no disponer de estos elementos, dibujar un boceto del sistema incluyendo los puertos y cables de tal manera que sea posible reconstruir y validar la escena posteriormente.

- Si está permitido, examinar todos los elementos circundantes donde pueda encontrarse información valiosa como contraseñas; elementos tales como notas, papeles, libretas o dispositivos móviles.

Se debe considerar también las personas que pueden encontrarse en el lugar del incidente previendo que no se presenten agresiones físicas, enfrentamientos o agresiones de cualquier tipo. En general se deben considerar los riesgos de

intervenir la escena dependiendo de las personas que puedan estar presentes en el momento de realizar la diligencia.

4.2.5.2 Personal involucrado. Se debe asegurar que el primer respondiente tenga capacidad de demostrar que tiene suficientes conocimientos técnicos y legales para realizar las labores mencionadas en los apartados anteriores, incluyendo las labores de manejo de la evidencia. Tener acceso a las mejores herramientas no garantiza la calidad de la evidencia digital si no va acompañada de conocimiento del respondiente. La adquisición de estos conocimientos es responsabilidad tanto del funcionario como de la empresa.

4.2.5.3 Documentación. La documentación es crítica cuando se requiere gestionar dispositivos digitales que presumiblemente contengan evidencia. El primer respondiente deberá tener en cuenta los siguientes puntos:

- Toda actividad realizada debe ser documentada. Esto asegura que no se ha dejado a un lado ningún detalle del proceso, lo cual puede ser de gran utilidad en caso que la evidencia vaya a ser valorada por terceros.

- El primer respondiente debe prestar especial atención a las trazas de fecha y hora de la evidencia. Se debe establecer una fuente de comparación para la fecha y hora la cual pueda ser aceptada y monitoreada por las partes.

- Deberá documentar cualquier evidencia visible en pantalla incluyendo programas y procesos activos así como los nombres de los documentos abiertos. Aquí se debe incluir una descripción de cualquier programa sospechoso de estar disfrazado como software conocido.

- Cualquier movimiento de la evidencia deberá ser documentado según la reglamentación local.

- Todos los dispositivos que potencialmente puedan contener evidencia y sus partes asociadas deberán estar marcados con sus números seriales o con una numeración única.

4.2.6 Elaboración de procedimientos. La elaboración de procedimientos adecuados y pertinentes es una pieza fundamental para el cumplimiento de los estándares internacionales en relación con la recolección y administración de evidencia digital. Se deben definir con claridad las operaciones y funciones que vaya a desarrollar la unidad de computación forense, así como el personal que la componga, incluyendo una descripción del trabajo que realizará, los requerimientos de cualificación y la estructura organizativa, entre otros aspectos. Administrativamente se debe considerar el licenciamiento del software a utilizar, la asignación y ubicación de los recursos necesarios y un programa de capacitación y actualización de conocimientos de las personas involucradas.

Se deben establecer directrices para la recepción y aceptación de solicitudes de revisión de evidencia digital. Estas directrices deben incluir formatos, puntos de contacto, documentación, criterios de aceptación y requerimientos para el envío de evidencia. Una vez una solicitud de servicio es aprobada, deben existir criterios para priorizar los casos y asignar el personal idóneo.

Los procedimientos deben ser probados antes de su implementación para asegurar que los resultados obtenidos puedan ser reproducidos por terceros. En la elaboración y validación de los procedimientos se debe documentar e incluir:

- Identificar las tareas o problemas a resolver.
- Proponer posibles soluciones.
- Probar cada solución en un ejemplo conocido y controlado.
- Evaluar los resultados de la prueba.
- Finalizar el procedimiento.

4.3 MARCO INSTITUCIONAL DE PTESA

A continuación se presentan los elementos conceptuales constitutivos de la empresa PTESA donde se realizó el trabajo de grado los cuales fueron tenidos en

cuenta durante la elaboración del procedimiento, procurando ajustarse a las normas internacionales sin dejar de lado los principios rectores de la compañía.

Misión

Facilitar la consecución de los objetivos de negocios a nuestros clientes ofreciéndoles soluciones tecnológicas confiables de alta calidad.

Visión

Continuar siendo los primeros en desarrollar e implementar soluciones de alta calidad como respuesta a la continua evolución de las transacciones electrónicas; cumpliendo con todos los requerimientos que exigen nuestros clientes y el mercado bajo los más rigurosos estándares de calidad internacional.

Principio Fundamental

LA COMPAÑÍA tiene como principio fundamental ofrecer soluciones tecnológicas de vanguardia, bajo un esquema de negociación ético en el que se beneficien todas las partes involucradas.

Definición del Negocio

Somos los mejores en:

- Desarrollar generadores de transacciones
- Optimizar autorizaciones
- Desarrollar negocios transaccionales

Lo que nos apasiona:

- Mejorar la calidad de vida de las personas

- Resolver los “puntos de dolor” en las transacciones.

Objetivos

- Maximizar el volumen transaccional que pasa por nuestros sistemas

- Maximizar la proporción de valor agregado capturado en el proceso de una transacción

Valores y Creencias

Todas las personas de esta organización tienen el potencial de ser **líderes.**

La efectividad de mis colegas depende de mí retribución **responsable.**

Una comunidad que se **apoya** prospera.
La **transparencia** genera confianza en los clientes y me permite obtener información valiosa.

La **confianza** es la base para hacer negocios exitosos y para establecer relaciones a largo plazo.

Mi retribución depende de mí **aporte.**

El **respeto** es la base para establecer relaciones de colaboración.

Solo siendo curiosos podemos **innovar** y satisfacer a nuestros clientes.

4.4 POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN DE PTESA

Las políticas de seguridad de la información definidas por PTESA, incluyen lineamientos generales en relación con el tratamiento de incidentes de seguridad, orientados a mantener a la alta gerencia enterada del estado actual de la empresa en temas de seguridad de la información. Sin embargo, se hace necesario establecer de manera más detallada la manera como esas políticas deben ser aplicadas por los funcionarios a nivel técnico y operacional.

Así por ejemplo, en las políticas se define que debe existir un Comité de Seguridad de la información, sus funciones y composición, señalando que el conducto regular para reportar los incidentes de seguridad debe ser a través del Responsable de Seguridad de la Información o uno de sus delegados, quien también podrá contar con el apoyo de la Dirección de Tecnología. No obstante, una vez se han reportado los incidentes, no se definen con claridad directrices sobre acciones que se deban tomar posteriormente.

En las políticas también se determina la responsabilidad de todos los empleados de la compañía en colaborar con el aseguramiento de los activos de información. Dado que la mayoría de las personas no cuenta con conocimientos técnicos en las TI, se torna difícil la identificación de vulnerabilidades y el reporte de las sospechas que les pueda generar determinada situación. La creación y consolidación de un grupo de respuesta a incidentes que sea conocido por todos los funcionarios y que esté al alcance de ellos, facilitará este proceso de identificación y reporte de incidentes de seguridad.

5. DISEÑO METODOLÓGICO

5.1 ENFOQUE DE LA INVESTIGACIÓN

Empírico-Analítico: se escogió debido al enfoque técnico y práctico del trabajo, así como la utilización de técnicas de observación de los distintos procesos dentro de la empresa y de compararlos frente a las mejores prácticas de la industria en relación con el manejo de incidentes y de la evidencia digital.

5.2 LÍNEA DE INVESTIGACIÓN

Línea de la investigación de la especialización: Computación Forense.

5.3 TÉCNICAS DE RECOLECCIÓN DE INFORMACIÓN Y ELABORACIÓN DEL TRABAJO DE GRADO

A continuación se presenta una visión general de los pasos que se llevaron a cabo durante el proceso de elaboración del presente trabajo:

- Se analizó el contenido de normas nacionales e internacionales relacionadas con la seguridad de la información, informática forense, grupos de respuesta a incidentes de seguridad informática, procesos de identificación, recolección y almacenamiento de evidencia digital y procedimientos de cadena de custodia.

- Se definió un extracto de las mejores prácticas y procesos aplicables a la recolección y administración de evidencia forense aplicada a los sistemas de las áreas administrativas y de desarrollo de software de la empresa PTESA, en consonancia con la normatividad legal colombiana vigente.

- Se elaboró un procedimiento de recolección y manejo de evidencia forense siguiendo las mejores prácticas identificadas durante el análisis, siguiendo un ordenamiento jerárquico en los documentos generados.

- Se socializaron los resultados del trabajo realizado ante el área gerencial y administrativa de la empresa PTESA.

6. RESULTADOS OBTENIDOS

Con base en los estándares internacionales establecidos por la industria de las tecnologías de la información en relación con la seguridad informática, y teniendo en cuenta el cuerpo normativo colombiano relacionado con la seguridad de la información, y habiendo identificado un punto de mejora en los procesos respectivos llevados a cabo actualmente en la empresa PTESA, se generó un procedimiento para la captura y gestión de evidencia forense de acuerdo a las necesidades detectadas en las áreas administrativa y de desarrollo de software de la compañía, el cual consta de varios documentos que cubren diversos tópicos. A continuación se presenta una descripción breve de cada uno de esos documentos y una referencia al documento completo que se incluye como anexo.

- Procedimiento para la captura y gestión de evidencia forense en equipos de cómputo de las áreas administrativa y de desarrollo de software de PTESA. Es el documento principal que articula todos los demás, en el cual se describen de forma sistemática las actividades tendientes a capturar y administrar de manera adecuada información forense que pueda ser de utilidad en un proceso legal o disciplinario manteniendo los principios de originalidad, integridad y admisibilidad de la evidencia. Ver Anexo M. Procedimiento para captura y gestión de evidencia forense en equipos de cómputo de las áreas administrativa y de desarrollo de software de PTESA.

- Bitácora de incidentes de seguridad. Es un formato que contiene información relevante para llevar el historial de incidentes de seguridad informática, en el cual se lleva un registro a través del tiempo de los incidentes reportados por los diferentes actores que tienen alguna asociación con la organización en relación con la seguridad informática con el fin de proporcionar una herramienta de análisis y control. Este documento sirve de insumo para el documento mencionado a continuación. Ver Anexo B. Bitácora de incidentes de seguridad

- Instructivo para diligenciar la bitácora de incidentes de seguridad. Contiene un manual paso a paso que indica qué información se debe registrar en la bitácora, presentando una descripción de cada uno de los campos que la componen y los criterios de evaluación que se deben tener en cuenta en el momento de definir el nivel de criticidad de los incidentes reportados. Ver Anexo F. Instructivo para diligenciar la bitácora de incidentes de seguridad informática.

- Acta de Esterilización de Medios de Almacenamiento. Formato en el que se registran las características de los medios de almacenamiento que son esterilizados en el cual se detallan también los resultados generados por las herramientas tecnológicas utilizadas. Este documento sirve de insumo para el documento mencionado a continuación. Ver Anexo A. Acta de esterilización de medios de almacenamiento.

- Instructivo para esterilización de medios de almacenamiento. Documento en el que se describen paso a paso las actividades que se deben llevar a cabo para lograr que un medio de almacenamiento pueda ser considerado estéril desde la perspectiva de la informática forense. Ver Anexo H. Instructivo para esterilización de medios de almacenamiento.

- Formato de Reporte de Incidentes de Seguridad. Formato que debe ser diligenciado por el miembro del grupo ERISI que recibe el reporte de un incidente de seguridad en el cual es posible determinar con claridad, el momento, lugar, naturaleza, características y personas relacionadas con el incidente que se reporta. Ver Anexo D. Formato para reporte de incidente de seguridad informática.

- Instructivo para reporte de incidentes de seguridad. Documento en el que se describen paso a paso las actividades que se deben llevar a cabo para diligenciar el formato de reporte de incidentes describiendo cada uno de los campos que lo componen. Ver Anexo K. Instructivo para reporte de incidentes de seguridad.

- Formato de Inventario Medios Almacenamiento. Documento donde se lleva el registro de los medios de almacenamiento que son recolectados en el desarrollo de un proceso de investigación forense cuando es necesario transportarlos o almacenarlos mientras se extraen de ellos imágenes forenses. Este mismo formato es utilizado por el área de tecnología para llevar el registro del inventario de dispositivos de almacenamiento de la compañía. Ver Anexo C. Formato de inventario de medios de almacenamiento.

- Instructivo para recolección de datos volátiles. Este instructivo contiene las acciones que se deben llevar a cabo con el fin de asegurar la recolección de los datos volátiles de un equipo de cómputo que funciona con sistema operativo Windows XP, Windows Vista, Windows 7 y/o Windows 8. Ver Anexo I. Instructivo para recolección de datos volátiles.

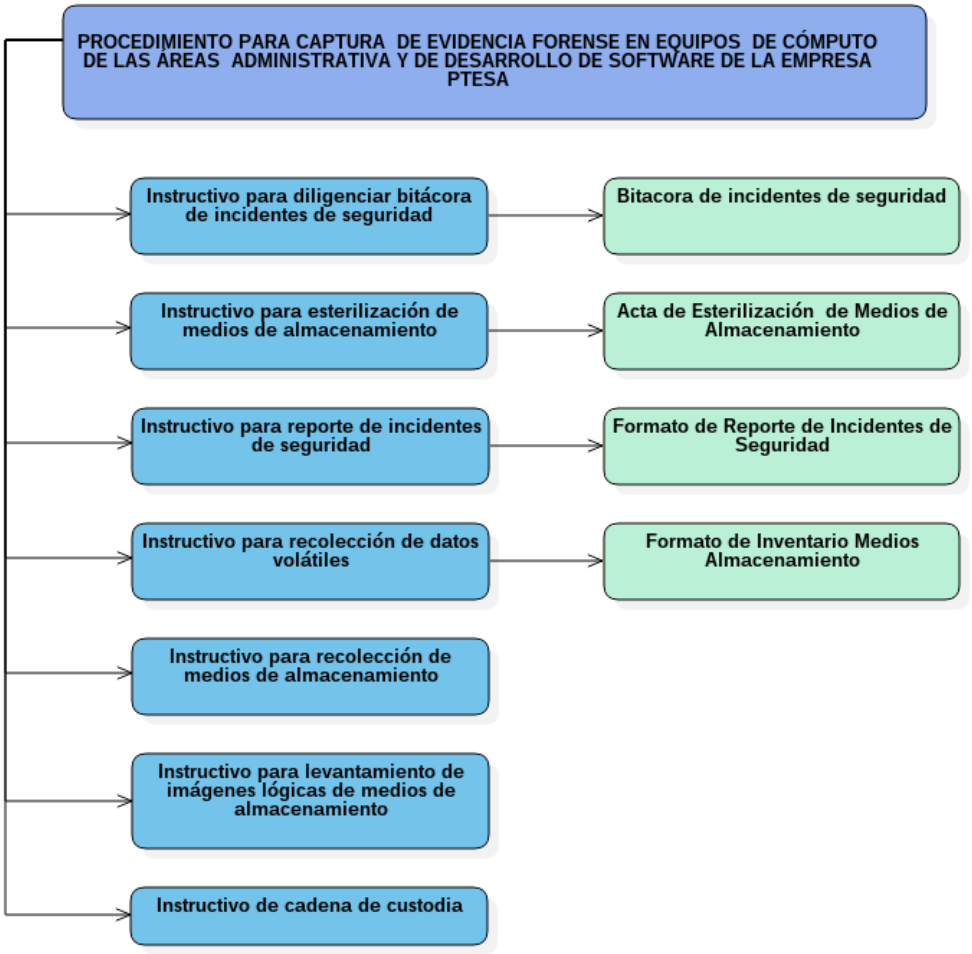
- Instructivo para recolección de medios de almacenamiento. Documento que indica las acciones que se deben ejecutar cuando se quiere hacer un inventario de medios de almacenamiento de datos en formato digital que van a ser puestos bajo cadena de custodia para ser utilizados en un proceso de investigación de informática forense. Ver Anexo J. Instructivo para recolectar medios de almacenamiento de datos.

- Instructivo para extracción de imágenes forenses de medios de almacenamiento. Este procedimiento permite obtener una copia bit a bit de los datos contenidos en un medio de almacenamiento de datos con el fin de utilizar la copia como evidencia forense del contenido del medio de almacenamiento original sin que este quede fuera de servicio, utilizando para ello un equipo con sistema operativo Microsoft Windows y una herramienta de software especializada. Ver Anexo G. Instructivo para extracción de imágenes forenses de medios de almacenamiento.

- Instructivo de cadena de custodia. Este documento indica los pasos que se deben llevar a cabo desde el momento en que un elemento entra en cadena de custodia al interior de la organización hasta el momento actual, con el fin de asegurar que la evidencia permanezca inalterada y así no pierda valor probatorio en un eventual proceso administrativo o judicial. Ver Anexo E. Instructivo de cadena de custodia.

A continuación se muestra un esquema de los documentos generados y las relaciones existentes entre ellos.

Figura 1. Esquema de documentos elaborados.



Fuente propia del autor.

Durante el desarrollo del proyecto y en concordancia con los esfuerzos impulsados por el gobierno nacional a través del documento CONPES 3701, se estableció la necesidad de conformar un grupo CERT en la empresa PTESA que esté encargado de gestionar los incidentes de seguridad que se presentan en la organización y que en consecuencia, lleve a cabo de forma adecuada y pertinente las actividades definidas en el procedimiento elaborado.

Dicho grupo se denominó ERISI o Equipo de Respuesta a Incidentes de Seguridad Informática, cuyas funciones y características se describen en el documento Manual de funciones del equipo de respuesta a incidentes de seguridad informática, en el cual se describen los antecedentes que se tuvieron en cuenta para su formación, adiciones a las políticas de seguridad de la empresa, una descripción de las

funciones que deberá cumplir, la estructura organizativa y las competencias de los funcionarios que lo compongan.

Todos estos documentos quedarán bajo la tutela del Comité de Seguridad de la Información de PTESA, con el conocimiento de la alta gerencia de la compañía, el cual será el encargado de su revisión, aprobación y actualización.

7. CONCLUSIONES

La legislación colombiana relacionada con la seguridad informática se ha ido actualizando paulatinamente durante los últimos años, proporcionando herramientas jurídicas que permiten proteger tanto los valiosos activos de información de las entidades públicas y privadas, como los derechos de los individuos. Parte de esa actualización incluye la aprobación de normas orientadas al aseguramiento de las evidencias digitales y la definición de mecanismos que faciliten la aplicación de esas normas como es el caso de los decretos reglamentarios, las sentencias aclaratorias y las modificaciones de las leyes vigentes relacionadas con el tema de este trabajo.

Existen en el ámbito tecnológico numerosas normas, principios, estándares y certificaciones emitidas por diversas entidades nacionales e internacionales que orientan a las empresas como PTESA en el conocimiento, evaluación y aplicación de las mejores prácticas de la industria en relación con el aseguramiento de la información. No obstante, por diversas razones, no siempre se aprovechan esos conocimientos pues no se toma el tiempo y el esfuerzo necesarios para su implementación en las organizaciones.

De acuerdo con la experiencia obtenida a través de los esfuerzos del gobierno colombiano en el fortalecimiento de los mecanismos de seguridad de la información en el país y a través del desarrollo del presente trabajo de grado, se hace evidente que uno de los primeros pasos que se deben adelantar para lograr un sistema de seguridad de la información fiable y eficaz es el establecimiento de grupos de respuesta a incidentes de seguridad, como la base para la implementación de otros mecanismo más sofisticados tales como los relacionados con la identificación, adquisición, recolección y análisis de evidencia digital.

Los principios de cadena de custodia son transversales a todos los procesos que tienen que ver con la evidencia forense y se requieren conocimientos técnicos apropiados para la adecuada aplicación de ellos en los procesos de gestión de incidentes de una compañía que esté interesada en la identificación, recolección y utilización de elementos de evidencia digital con valor probatorio en eventuales procesos disciplinarios y penales a que haya lugar cuando ocurren incidentes de seguridad de la información.

8. RECOMENDACIONES

Una vez entregada la documentación producto del presente trabajo de grado a la empresa PTESA y realizada la socialización del mismo con el personal de las áreas de gerencia y administración, se recomienda la revisión, evaluación y aprobación del procedimiento de captura y gestión de evidencia forense y del manual de funciones del grupo ERISI.

Una vez aprobada la viabilidad y pertinencia del contenido de los documentos en mención, se recomienda la aplicación de los mismos mediante la constitución del grupo de respuestas a incidentes de seguridad, la asignación de recursos económicos y de personal necesarios para su funcionamiento.

Se recomienda también establecer un programa continuado de formación y capacitación en temas de seguridad de la información para el personal asignado al grupo ERISI, así como un programa de concienciación sobre la necesidad de reportar de forma oportuna los incidentes de seguridad que se identifiquen, orientado a todos los empleados de la compañía.

Finalmente se recomienda asegurar la actualización, complementación y constante verificación de la documentación que es entregada dado que tanto la legislación como los estándares y normas internacionales están en constante evolución, procurando adaptarse a las siempre crecientes amenazas a la seguridad de la información.

BIBLIOGRAFÍA

COBB, Chey. How to secure the chain of custody in a digital forensics investigation [online]. SearchITChannel. Diciembre 2007. Disponible en <http://searchitchannel.techtarget.com/tip/How-to-secure-the-chain-of-custody-in-a-digital-forensics-investigation>

COLOMBIA. CONGRESO DE LA REPUBLICA. Ley 1712 (6, marzo, 2014). Por medio de la cual se crea la ley de transparencia y del derecho de acceso a la información pública nacional y se dictan otras disposiciones [online]. Bogotá D.C.: El Ministerio, 2014. Disponible en <http://www.mintic.gov.co/portal/604/articles-7147_documento.pdf>

CONGRESO DE COLOMBIA. Ley 906 (1, septiembre, 2004). Por la cual se expide el Código de Procedimiento Penal. (Corregida de conformidad con el Decreto 2770 de 2004) [online]. Bogotá D.C.: El Ministerio, 2004. Disponible en <http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=14787>

COLOMBIA. CONSEJO NACIONAL DE POLÍTICA ECONÓMICA Y SOCIAL. LINEAMIENTOS DE POLÍTICA PARA CIBERSEGURIDAD Y CIBERDEFENSA [online]. Bogotá D.C. (14, julio, 2011). Disponible en <http://www.mintic.gov.co/portal/604/articles-3510_documento.pdf>

COLOMBIA. DEPARTAMENTO NACIONAL DE PLANEACION. El Consejo Nacional de Política Económica y Social, CONPES [online]. Actualizado 29 de mayo de 2015. Disponible en <https://www.dnp.gov.co/CONPES/Paginas/conpes.aspx>

COLOMBIA. FISCALÍA GENERAL DE LA NACIÓN. Continuación de la Resolución 0-6394. (22, diciembre, 2004). Por medio de la cual se adopta el Manual de Procedimientos del sistema de cadena de custodia para el sistema penal acusatorio [online]. Página 19. Disponible en <http://www.usergioarboleda.edu.co/derecho_penal/pdf/2004-MANUAL CADENA DE CUSTODIA.pdf>

COLOMBIA. PRESIDENTE DE LA REPÚBLICA. Decreto 1377 (27, junio, 2013). Por el cual se reglamenta parcialmente la Ley 1581 de 2012 [online]. Diario Oficial. Bogotá, D. C., 2013. Disponible en http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=53646

COLOMBIA. PRESIDENTE DE LA REPÚBLICA. Ley 1581 (17, octubre, 2012). Por la cual se dictan disposiciones generales para la protección de datos personales [online]. Diario Oficial. Bogotá, D. C., 2012. Disponible en <http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=49981>

CONGRESO DE COLOMBIA. Ley 1273 (5, enero, 2009). Por medio de la cual se modifica el código penal, se crea un nuevo bien jurídico tutelado denominado “de la protección de la información y de los datos” y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones [online]. Bogotá D.C.: El Ministerio, 2009. Disponible en <http://www.mintic.gov.co/portal/604/articles-3705_documento.pdf>

CONGRESO DE COLOMBIA. Ley 527 (18, agosto, 1999). Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones [online]. Bogotá D.C.: El Ministerio, 1999. Disponible en http://www.archivogeneral.gov.co/sites/all/themes/nevia/PDF/Transparencia/LEY_527_DE_1999.pdf

CONGRESO DE COLOMBIA. Ley 599 (24, julio, 2000). Por la cual se expide el Código Penal [online]. Bogotá D.C.: El Ministerio, 2000. Disponible en < http://www.archivogeneral.gov.co/sites/all/themes/nevia/PDF/Transparencia/Codigo_Penal.pdf>

Corporación Colombia Digital. Perspectiva de la Seguridad Informática en Latinoamérica. Colombia Digital [online]. Julio 2, 2014. Disponible en <http://colombiadigital.net/actualidad/noticias/item/7289-perspectiva-de-la-seguridad-informatica-en-latinoamerica.html>

INTERNATIONAL STANDARD ISO/IEC 27037. Information technology — Security techniques — Guidelines for identification, collection, acquisition, and preservation of digital evidence. Primera edición. 2012. Página 6

NOBLETT, Michael; POLLITT, Mark y PRESLEY, Lawrence. Recovering and Examining Computer Forensic Evidence [online]. Forensics Science Communications. Volume 2. Number 4. Octubre 2000. Disponible en <http://www.fbi.gov/about-us/lab/forensic-science-communications/fsc/oct2000/computer.htm/>

THE FIRST DIGITAL FORENSIC RESEARCH WORKSHOP (DFRWS). A Road Map for Digital Forensic Research [online]. Technical Report. DTR - T001-01 FINAL. Utica, New York, August 7-8, 2001. November 6th, 2001 – Final. Disponible en <http://www.dfrws.org/2001/dfrws-rm-final.pdf>

THE FIRST DIGITAL FORENSIC RESEARCH WORKSHOP (DFRWS). INTERNATIONAL ORGANIZATION ON DIGITAL EVIDENCE (IOCE). Digital Evidence: Standards and Principles [online]. Volume 2. Number 2. Abril 2000. Disponible en <http://www.fbi.gov/about-us/lab/forensic-science-communications/fsc/april2000/swgde.htm/>

UNION INTERNACIONAL DE TELECOMUNICACIONES. Decisiones destacadas de Guadalajara [online]. Ciberseguridad. Noviembre 2010. Disponible en <https://www.itu.int/net/itunews/issues/2010/09/20-es.aspx>

ANEXO A. ACTA DE ESTERILIZACIÓN DE MEDIOS DE ALMACENAMIENTO

Fecha Hora (AAAA/MM/DD hh:mm p)	
Nombre del funcionario:	
Objetivo:	
DESCRIPCIÓN DEL DISPOSITIVO	
Tipo de medio de almacenamiento:	
Capacidad total de almacenamiento:	
Serial:	
Marca:	
Herramienta de Software:	
Reporte generado por la herramienta:	
Reporte de fallos:	
Firma del funcionario:	

Fuente: propio del autor.

ANEXO B. BITACORA DE INCIDENTES DE SEGURIDAD

No.	Fecha/ Hora	Reportado por	Área que reporta	Evaluado por	Activo de información	Criticidad	Detalles

Fuente: propio del autor.

ANEXO C. FORMATO DE INVENTARIO DE MEDIOS DE ALMACENAMIENTO

INFORMACIÓN GENERAL	
Fecha/Hora (AAAA/MM/DD hh:mm p)	
Nombre del funcionario:	

DATOS DEL RESPONSABLE DEL DISPOSITIVO	
Nombre completo:	
Cargo:	
Área:	
Descripción del computador:	

DATOS DEL DISPOSITIVO	
Tipo de medio de almacenamiento:	
Número Serial:	
Marca:	
Capacidad de almacenamiento:	

Elaborado por:	**Revisado por:**	**Aprobado por:**
GUILLERMO ÁLVAREZ Fecha: Noviembre de 2015		

Fuente: propio del autor.

ANEXO D. FORMATO PARA REPORTE DE INCIDENTE DE SEGURIDAD INFORMÁTICA

DATOS PERSONALES

Ingrese en esta parte los datos personales de la persona que está reportando el incidente.

Nombre completo:	
Cargo:	**Área:**
Correo electrónico:	
Teléfono interno:	**Teléfono particular:**

INFORMACIÓN SOBRE EL INCIDENTE

La información que usted proporcione acerca del incidente ayudará a dar solución de una mejor y más rápida forma.

Fecha y hora en que se suscitó el incidente:

Marque con una X las opciones aplicables al incidente

	Uso indebido de información.		**Cambio en la configuración de un equipo.**
	Uso inadecuado de recursos informáticos.		**Ataque o infección de malware, o código malicioso (virus, gusanos, troyanos, etc.)**
	Divulgación no autorizada de información personal		**Acceso o intento de acceso sin autorización a un sistema informático.**
	Acceso o intento de acceso físico no autorizado.		**Pérdida o destrucción no autorizada de información.**
	Ingeniería social.		**Interrupción en los servicios de comunicaciones.**
	Uso indebido de correo electrónico institucional.		**Anomalía o vulnerabilidad técnica del software.**
	Modificación de información de un sitio o página Web.		**Robo o pérdida de equipo.**
	Robo o pérdida de información.		**Amenaza o acoso por medio electrónico.**
	Modificación, instalación o eliminación de software.		**Otro:**

DESCRIPCIÓN DEL INCIDENTE

Brevemente describa y proporcione información acerca del incidente

Detección del incidente				
Describa brevemente cómo se detectó el incidente				
El incidente aún está en progreso	**Sí**		**No**	
Tiempo aproximado de duración del incidente:				

INFORMACIÓN SOBRE EL ACTIVO O BIEN AFECTADO

Si conoce la información, llene los campos acerca de la información concerniente al bien afectado.

Descripción del activo o bien:
Localización física:
Nombre y área del funcionario que tiene a cargo el recurso afectado

¿Existe una copia o respaldo de la información?	**Sí**		**No**	
¿El recurso afectado es responsabilidad directa de la organización?	**Sí**		**No**	
¿El recurso afectado tiene conexión a internet?	**Sí**		**No**	
Sistema Operativo:				
Firmas				

Elaborado por:	**Revisado por:**	**Aprobado por:**
GUILLERMO ÁLVAREZ Fecha: Noviembre de 2015		

Fuente: propio del autor.

ANEXO E. INSTRUCTIVO DE CADENA DE CUSTODIA

OBJETIVO

Los registros de cadena de custodia permiten hacer un seguimiento, en todo momento, de todo elemento de evidencia, con el fin de asegurar que permanezca inalterada y así no pierda valor probatorio en un eventual proceso administrativo o judicial. Este documento indica los pasos que se deben realizar desde el momento en que un elemento de evidencia entra en cadena de custodia al interior de la organización hasta el momento actual.

GLOSARIO

Bitácora: Medio escrito donde se registran anotaciones que se consideran útiles para el seguimiento de una serie de eventos.

Cadena de custodia. Procedimiento de control que se aplica a elementos de evidencia desde su recolección hasta el final de su vida útil y que tiene como fin evitar alteraciones o cualquier contaminación o destrucción.

Embalar. Empaquetar o colocar un objeto adecuadamente en un envoltorio con el fin de transportarlo.

ERISI. Siglas de Equipo de Respuesta a Incidentes de Seguridad Informática. Se refiere al grupo de personas dentro de la empresa encargado de evaluar, documentar y gestionar los incidentes de seguridad informática.

Evidencia forense. Todo indicio que permite establecer a través de métodos científicos, una relación entre un crimen y la persona que lo cometió.

HASH. Función matemática que a través de la aplicación de un algoritmo permite obtener un código de longitud fija a partir de unos elementos de entrada de datos.

Imagen forense. Copia bit a bit de un medio de almacenamiento digital en la cual quedan grabados los datos tal y como se encuentran en el medio original.

USB. Iniciales en inglés de Puerto Serial Universal (Universal Serial Bus) que es un puerto de comunicación estándar utilizado en múltiples dispositivos que se pueden comunicar con un computador.

GENERALIDADES

La Resolución 0-2869 establece que "el Sistema de Cadena de Custodia debe asegurar las características originales de los elementos materia de prueba durante la protección de la escena, recolección, transporte, análisis, almacenamiento, conservación, preservación, recuperación y disponibilidad de éstos, identificando al responsable en cada una de sus etapas y que los elementos correspondan al caso investigado". Esta definición corresponde con la aplicación práctica de la normatividad colombiana en el tema en cuestión y por tanto arroja luz acerca de lo que se espera de la implementación de un sistema de cadena de custodia aceptable legalmente en el país.

En relación con el registro de evidencia, de acuerdo con la norma ISO IEC 27037:2012 en su apartado 6.1, en cualquier investigación de informática forense, el primer respondiente deberá estar en capacidad de registrar los datos y dispositivos adquiridos así como el momento en que estos entran en cadena de custodia. El propósito de tener estos registros es permitir identificar los movimientos y el acceso a la evidencia potencial en cualquier punto de tiempo; el registro puede involucrar más de un documento y debe contener como mínimo lo siguiente:

- Un identificador único de evidencia.
- Quién tuvo acceso a la evidencia, el momento y el lugar en que esto sucedió.
- Quién ingresó y extrajo la evidencia del repositorio establecido y cuándo sucedió.
- Por qué la evidencia fue extraída y la autoridad relevante si aplica.
- Cualquier cambio inevitable sobre la evidencia y el nombre del individuo responsable así como la justificación para la ocurrencia del cambio.

Por otra parte, en relación con los procesos de administración de evidencia, el Manual de Procedimientos del sistema de cadena de custodia establecido por la Fiscalía General de la Nación establece los siguientes factores críticos de éxito para no perder la trazabilidad de la cadena de custodia:

1. Utilizar contenedores estériles para almacenar la evidencia con el fin de asegurar y conservar las características de los elementos físicos de prueba.
2. En cada traspaso y traslado, el embalaje debe estar perfecto e íntegro, las bolsas no pueden presentar cortes.
3. El rótulo del elemento no debe presentar tachones o enmendaduras y debe

identificar plenamente el elemento. Éste documento no se debe retirar del embalaje en ningún momento.

4. El almacenamiento de los elementos físicos de prueba, debe ser en condiciones ambientales adecuadas para conservar las condiciones y características originales de los elementos físicos de prueba, contando con el espacio adecuado para que no se contaminen unos con otros.

5. El diligenciamiento del formato de cadena de custodia, se debe realizar de manera completa y organizada, sin presentar tachones o enmendaduras y debe identificar plenamente los traslados y traspasos, durante todo el proceso de cadena de custodia, en forma tal que se conozca la identidad de cada custodio y las acciones que realizó con el elemento.

En conclusión, existen normas y recomendaciones tanto nacionales como internacionales que se pueden tomar como referencia para la elaboración de mecanismos de cadena de custodia y que se deben aplicar para asegurar que los elementos de evidencia que están bajo la tutela de la empresa no pierdan valor probatorio.

ALCANCE

Las actividades descritas en este documento deberán ser ejecutadas por personal perteneciente al grupo ERISI, cada vez que un elemento de evidencia o de soporte documental es reportado por un miembro del mismo grupo como elemento de valor en un caso de investigación forense llevado a cabo al interior de la compañía. De igual manera deberá ser tenido en cuenta cuando se hace entrega de evidencia a terceros autorizados o cuando se reciben de terceros elementos con las características mencionadas, de tal forma que un elemento de evidencia cualquiera, pasa a ser responsabilidad de la compañía.

DESCRIPCIÓN DE ACTIVIDADES

RECOLECCIÓN DE ELEMENTOS DE EVIDENCIA

Las actividades descritas a continuación se llevarán a cabo cuando uno o más elementos ingresen por primera vez al sistema de cadena de custodia definido por la organización.

1. Todos los elementos físicos que entran a cadena de custodia deberán ser embalados y sellados individualmente en contenedores que se encuentren en buen estado, que

no presenten roturas ni abolladuras y que preferiblemente no hayan sido utilizados previamente.

Los dispositivos electrónicos que son susceptibles de descargas electrostáticas tal como ocurre con discos duros internos y otros similares, deberán ser embalados en contenedores no conductores de electricidad que los protejan del daño del dispositivo o alteración no intencionada del contenido del mismo, por la circulación no controlada e inesperada de corriente eléctrica en los circuitos que lo componen.

Si el elemento que se registra proviene de un tercero, se deberá verificar rigurosamente el cumplimiento de las ya mencionadas características de embalaje para continuar con el proceso de registro. De no ser así, el elemento será devuelto al tercero indicando por el conducto regular que se haya establecido, las razones por las que no se admite el elemento de evidencia por parte de la organización.

2. Se deberá etiquetar cada uno de los elementos utilizando el Formato de etiqueta de cadena de custodia que se encuentra al final de este punto, el cual deberá ser diligenciado como se describe a continuación.

- **Fecha/Hora de embalaje.** Indica la fecha y hora en que el elemento fue ingresado a cadena de custodia, incluyendo año, mes, día, hora, minuto y periodo horario (a.m. ó p.m.).

- **ID Caso.** Identificador del caso de investigación al que pertenece el elemento de evidencia como haya quedado registrado en la bitácora de incidentes de seguridad y construido siguiendo las reglas definidas en el procedimiento para captura de evidencia forense.

- **ID Elemento.** Número consecutivo asignado al elemento de evidencia que comienza en uno (1) y que es único para cada caso de investigación. Para poder determinar el número consecutivo que se debe asignar al elemento, el funcionario que realiza el procedimiento, deberá remitirse al documento de registro de elementos de evidencia del caso al que este pertenece, cuyo contenido se especifica detalladamente en el paso tres (3) de este instructivo.

- **Nombre.** Nombre completo del miembro del grupo ERISI que realiza el procedimiento de ingreso del elemento a cadena de custodia. De ser posible, se recomienda incluir el nombre de un testigo que esté observando el desarrollo del procedimiento el cual no necesariamente deberá pertenecer al grupo ERISI.

- **Lugar.** Se deberá indicar la ubicación física donde el elemento al cual corresponde la etiqueta fue recolectado como evidencia e ingresado a cadena de custodia.

- **Firma.** Firma del miembro del grupo ERISI que realiza el procedimiento. Si se incluyó el nombre de un testigo, en este campo deberá incluirse su firma.

Al diligenciar los datos de la etiqueta, especialmente si se hace a mano alzada, el funcionario que realiza el procedimiento deberá asegurarse de utilizar letras y números claros que no generen ambigüedad o confusión como puede ocurrir en el caso de no poder distinguir un número seis (6) de la legra G mayúscula o el número uno (1) de una vocal i mayúscula (I) o de la letra ele minúscula (l).

Una vez diligenciada la etiqueta, esta deberá ser adherida al envoltorio en que fue almacenado el elemento que se ingresa a cadena de custodia y cubierta con un material aislante (por ejemplo cinta de embalaje) con el fin de evitar alteraciones como adiciones, tachaduras o el simple deterioro de la etiqueta, producto del paso del tiempo y de las condiciones mismas de los elementos físicos que la conforman.

El formato de la etiqueta es como se muestra en la tabla a continuación.

FORMATO DE ETIQUETA DE CADENA DE CUSTODIA	
Fecha/hora embalaje:	
Id caso:	
Id elemento:	
Nombre:	
Lugar:	
Firma:	

El grupo ERISI deberá contar con una cantidad suficiente de etiquetas de este tipo para que estén disponibles en cualquier momento y puedan ser utilizadas en una emergencia. Sin embargo, de ser posible, se recomienda diligenciar la etiqueta en un editor de textos durante la ejecución del procedimiento e imprimirla para continuar con los pasos ya descritos.

3. Con el fin de garantizar el seguimiento a cada elemento que es ingresado a cadena de custodia, su relación con un caso de investigación y con otros elementos de evidencia, como parte del proceso de registro se debe diligenciar un documento que contenga los siguientes datos:

- **Número del caso al que pertenece.** Si se incluye la información de varios elementos asociados al mismo caso en un solo documento, se deberá incluir este dato una sola vez en el encabezado de cada hoja que lo conforma.

- **Número del elemento.** Identificador único, en serie y en orden secuencial de los elementos de evidencia o de gestión documental asociados al mismo caso de investigación.

- **Fecha y hora** en que el elemento ingresó a cadena de custodia, incluyendo año, mes, día, hora, minuto y periodo horario (a.m. ó p.m.).

- **Nombre del funcionario.** Nombre completo del miembro del grupo ERISI que hizo la recolección de la evidencia o que recibió de un tercero los elementos de evidencia.

- **Descripción.** Descripción del elemento que se está ingresando en cadena de custodia. Por ejemplo: Memoria USB color negro de marca Kingston. Se deben indicar aquí características físicas relevantes que permitan diferenciar a simple vista un elemento de otro.

- **Motivo.** Descripción de la motivación que llevó al funcionario a recolectar la evidencia o a poner un documento en cadena de custodia. De ser posible se debe incluir un sustento legal, de cumplimiento de políticas de seguridad de la empresa o de cumplimiento de procesos o estándares definidos por la empresa por el cual se hizo la recolección del elemento.

- **Lugar.** Permite determinar la ubicación física del elemento en el momento en que se llevó a cabo la recolección. Si el elemento que ingresa proviene de un tercero, en este campo se indicará su nombre del tercero de quien se recibe la evidencia y el rol desempeñado por él en el caso de investigación forense que se está adelantando en la organización.

- **Acción.** Descripción detallada de la manera cómo se realizó la recolección del elemento. Se puede referenciar en este punto a otro documento en cuyo caso, el tal deberá también ser ingresado en cadena de custodia. Si el elemento se recibe de un

tercero, se deberá indicar directamente o por referencia a otro documento las actividades ejecutadas por el tercero sobre el elemento que es ingresado en cadena de custodia durante el proceso de recolección y se debe anexar documento firmado por él donde se deja constancia de tales acciones.

- **Controles.** En esta sección se deberán indicar los mecanismos aplicados al elemento por los cuales es posible determinar su integridad. En el caso de imágenes forenses por ejemplo, se deberá indicar aquí el valor del HASH y/o código de verificación de errores calculado para la imagen que está contenida en el elemento de evidencia que se ingresa en cadena de custodia y el nombre del algoritmo utilizado. En caso de recibir el elemento de parte de un tercero, se deberá verificar la validez y cumplimiento de los controles mencionados antes de recibirlo formalmente.

- **Testigo.** Si durante el proceso de recolección estaba presente un testigo, se deberá indicar su nombre y rol que desempeña al interior de la organización o su relación con el caso de investigación si se trata de un tercero.

- **Firmas.** Firma del funcionario o funcionarios que participaron en la elaboración, revisión y/o aprobación del documento.

GESTIÓN DE LOS ELEMENTOS DE EVIDENCIA

Las actividades descritas a continuación se llevarán a cabo cuando uno o más elementos que están bajo el sistema de cadena de custodia de la organización son trasladados, manipulados, o transferidos de una persona a otra o de funcionarios de la organización a terceros debidamente autorizados.

Se deberá generar un documento donde se especifique, para cada elemento sobre el cual se realice alguna de las actividades de gestión mencionadas anteriormente, la siguiente información:

- **Número del caso al que pertenece**. Si se incluye la información de varios elementos asociados al mismo caso en un solo documento, se deberá incluir este dato en el encabezado de cada hoja que compone el documento.

- **Número del elemento**. Identificador único, en serie y en orden secuencial de los elementos de evidencia o de gestión documental asociados al mismo caso de investigación y que están siendo objeto de las mismas acciones de gestión.

- **Fecha y hora** en que se realizó la actividad de gestión sobre el elemento, incluyendo año, mes, día, hora, minuto y periodo horario (a.m. ó p.m.).

- **Nombre del funcionario responsable**. Nombre completo del funcionario bajo cuya responsabilidad se encuentra el elemento objeto de gestión. Si el elemento es recibido de un tercero habiendo estado previamente bajo la custodia de la empresa, en este campo se indicará su nombre y el rol llevado a cabo en el caso de investigación forense que se está adelantando.

- **Nombre del nuevo responsable**. Nombre completo del funcionario bajo cuya responsabilidad se deja el elemento objeto de gestión. Este dato se diligencia si el elemento cambia de responsable. Si el elemento es entregado a un tercero, en este campo se indicará su nombre y el rol asignado al tercero en el caso de investigación forense que se está adelantando en la organización.

- **Motivo**. Descripción de las razones por las que se lleva a cabo la actividad de gestión sobre el elemento que está en cadena de custodia. Aquí se debe indicar una fundamentación legal o procedimental que justifique la realización de la actividad de gestión sobre el elemento.

- **Lugar**. Permite determinar la ubicación física del elemento en el momento en que se llevó a cabo la acción de gestión.

- **Acción**. Descripción de la acción ejecutada sobre el elemento. Si se recibe de un tercero, se deberá indicar directamente o por referencia a otro documento las actividades ejecutadas por el tercero sobre el elemento y se debe anexar documento firmado y aceptado explícitamente por el tercero, donde se deja constancia de las acciones ejecutadas sobre la evidencia.

- **Controles**. En esta sección se deberán indicar los mecanismos aplicados al elemento por los cuales es posible determinar su integridad. Tanto el responsable al inicio de la actividad de gestión, como el nuevo responsable del elemento sobre el que se realiza, deberán realizar la verificación del cumplimiento de los controles aquí mencionados. En el caso de imágenes forenses por ejemplo, se deberá indicar aquí el valor del HASH y/o código de verificación de errores calculado para la imagen que está contenida en el elemento de evidencia y el nombre del algoritmo utilizado.

  Si los responsables pertenecen a la organización, la firma del documento generado implica la aceptación de las partes del cumplimiento de los controles. En caso que el nuevo responsable sea un tercero, deberá quedar constancia firmada donde se indique explícitamente que se realizó a satisfacción la verificación de los controles al oficializar la entrega del elemento.

- **Firmas**. Firma del funcionario o funcionarios que participaron en la elaboración, revisión y/o aprobación del documento.

Cada documento generado producto del presente instructivo o mencionado en él, deberá ser anexado al folio del caso de investigación junto con el reporte del incidente de seguridad que dio inicio al caso y la demás documentación relacionada.

Elaborado por:	**Revisado por:**	**Aprobado por:**
GUILLERMO ÁLVAREZ Fecha: Noviembre de 2015		

Fuente: propio del autor.

ANEXO F. INSTRUCTIVO PARA DILIGENCIAR LA BITÁCORA DE INCIDENTES DE SEGURIDAD INFORMÁTICA

OBJETIVO

La bitácora de incidentes de seguridad informática permite llevar un registro a través del tiempo de los incidentes reportados por los diferentes actores que tienen alguna asociación con la organización en relación con la seguridad informática con el fin de proporcionar una herramienta de análisis y control.

GLOSARIO

Bitácora: Medio escrito donde se registran anotaciones que se consideran útiles para el seguimiento de una serie de eventos.

ERISI: Abreviatura de Equipo de Respuesta a Incidentes de Seguridad Informática. Se refiere al grupo de personas dentro de la empresa encargado de evaluar, documentar y gestionar los incidentes de seguridad informática.

Impacto. Medida de las consecuencias que puede generar la materialización de una amenaza de seguridad.

Incidente de seguridad informática. Cualquier hecho que afecta o podría afectar la seguridad informática de la organización.

Matriz de riesgos. Herramienta de control donde se relacionan de forma ordenada los activos de información de una compañía y las vulnerabilidades, amenazas y riesgos a los que está expuesto cada uno de ellos asignándoles una valoración cualitativa o cuantitativa.

Seguridad de la información. Conjunto de normas preventivas y reactivas que se toman frente a los sistemas de información de una organización con el fin de resguardar y proteger las características de la información: integridad, confidencialidad y disponibilidad.

GENERALIDADES

Las bitácoras son elementos físicos donde se almacenan de forma sistemática todos los hechos que ocurren en un lugar, proceso o sistema cuyo seguimiento se desea registrar. Son utilizadas comúnmente en varios ámbitos, actualmente se usan también en el campo de la tecnología, puesto que permiten realizar investigaciones en caso de fallos o situaciones

catastróficas. Un ejemplo claro es la caja negra de un avión, la cual registra el comportamiento de todos los sistemas y las mediciones de los aparatos, de tal manera que cuando ocurre un desastre, es posible determinar las causas a través de los datos registrados en ella. De manera similar, una bitácora bien diligenciada en relación con los incidentes de seguridad de la información puede convertirse en una valiosa herramienta en una investigación forense. Sin embargo, dado que en el caso de la bitácora de incidentes de seguridad no se realiza de forma automática, su utilidad dependerá de la rigurosidad con que los responsables de ella diligencien los eventos ocurridos.

ALCANCE

El libro que contiene la bitácora deberá estar bajo la custodia del grupo ERISI, quien deberá velar por su integridad y disponibilidad. Además, de acuerdo con la política de seguridad de la compañía, el conducto regular para la notificación de incidentes es el grupo EIRIS y por lo tanto, las actividades descritas en este instructivo deberán ser realizadas por uno sus miembros cada vez que un incidente de seguridad es identificado o reportado.

DESCRIPCIÓN DE ACTIVIDADES

La bitácora es un libro cuyas hojas están numeradas para evitar que sean extraídas, de manera que al diligenciarla, se deberá respetar el orden asignado. El diligenciamiento deberá hacerse sin tachaduras ni enmendaduras, asegurándose de usar letra clara y legible.

A continuación se explica uno a uno los campos que la componen:

- **No**. Número consecutivo que permite identificar un reporte en particular durante el proceso de documentación y tratamiento dl incidentes.

- **Fecha/Hora**. Indica la fecha y hora en que el incidente fue registrado en la bitácora, incluyendo año, mes, día, hora, minuto y periodo horario (a.m. ó p.m.).

- **Reportado por**. Nombre del funcionario del grupo ERISI que reporta el incidente al grupo ERISI. Cuando se reporta el cierre de un caso iniciado por el reporte de un incidente, en este campo se registra el nombre del funcionario que hizo el tratamiento del caso.

- **Área que reporta**. Área de la empresa donde el incidente fue detectado. Si el reporte lo realiza un actor externo a la organización, se debe indicar el nombre en este campo. Si se trata del cierre de un caso, en este campo se debe indicar que es el grupo ERISI.

- **Evaluado por**. Nombre del funcionario que recibió el reporte y realizó el registro en la bitácora.

- **Criticidad**. Nivel de criticidad asignada al incidente inicialmente por el funcionario que recibe y registra el reporte. Cuando se trata del cierre de un caso, en este campo se debe indicar el nivel de criticidad final asignado al reporte durante su tratamiento.

- **Activo de información**. Nombre o código del activo de información tal como aparece en el inventario de activos de información de la compañía.

- **Detalles**. Breve descripción del incidente reportado. Cuando se trata del inicio o cierre de un caso iniciado por un incidente, en este campo se debe indicar esta situación junto con el número identificador del registro que inició el caso (cuando se trata de un cierre).

- **Firmas**. Firma del (los) funcionario(s) involucrados con el incidente.

CRITERIOS DE EVALUACIÓN

La evaluación del nivel de criticidad de un incidente se asignará teniendo en cuenta el impacto que esta puede tener sobre los activos de información de la compañía, tomando como base la matriz de riesgos de la organización, en la cual se hace una relación de cada uno de los activos, las vulnerabilidades que tienen, las amenazas que pueden llegar a explotar las vulnerabilidades y una estimación de la probabilidad de ocurrencia o materialización de las amenazas. A partir de esa información, en la matriz de riesgos se establece una valoración cuantitativa del nivel de impacto que puede llegar a tener, en cada una de las características de la información, integridad, confidencialidad y disponibilidad, la materialización de una amenaza.

Con base en la valoración definida en la matriz de riesgos, cuando se presenta un incidente de seguridad en uno de los activos de información registrados, se deberá determinar la valoración del impacto y así poder establecer la criticidad del incidente.

A continuación se describen los niveles de criticidad que pueden ser asignados a un incidente teniendo en cuenta que la matriz de riesgos está construida con una escala que va del 1 al 75 siendo uno (1) el valor que indica un menor impacto y setenta y cinco (75) el que indica el mayor impacto.

- **Bajo**. Se asigna para el nivel de impacto entre 1 y 10 significando que el incidente reportado no implica un riesgo para la seguridad de la información la empresa. Los

reportes que caben en esta clasificación suelen tratarse de malos entendidos o problemas resultantes del uso inadecuado de las herramientas informáticas.

- **Medio**. Se asigna para el nivel de impacto entre 11 y 35 significando que el incidente reportado no tiene el potencial de comprometer la continuidad del negocio pero cuyas implicaciones pueden afectar el adecuado desempeño de la empresa.

- **Medio Alto**. Se asigna para el nivel de impacto entre 36 y 65 significando que el incidente tiene el potencial de comprometer la continuidad del negocio y por tanto debe ser asignado rápidamente.

- **Alto**. Se asigna para el nivel de impacto entre 66 y 75 significando que el incidente compromete la continuidad del negocio y por tanto debe ser asignado inmediatamente.

Una vez se ha realizado el reporte del incidente en la bitácora, se procederá a asignarlo a uno de los miembros del grupo ERISI para su gestión.

Elaborado por:	**Revisado por:**	**Aprobado por:**
GUILLERMO ÁLVAREZ Fecha: Noviembre de 2015		

Fuente: propio del autor.

ANEXO G. INSTRUCTIVO PARA EXTRACCIÓN DE IMÁGENES FORENSES DE MEDIOS DE ALMACENAMIENTO

OBJETIVO

Este procedimiento permite obtener una copia bit a bit de los datos contenidos en un medio de almacenamiento de datos con el fin de utilizar la copia como evidencia forense del contenido del medio de almacenamiento original sin que este quede fuera de servicio, utilizando para ello un equipo con sistema operativo Microsoft Windows y una herramienta de software especializada.

GLOSARIO

Bit. Mínima unidad de medida utilizada en informática para representar 1 o 0 significando encendido o apagado y que se utiliza para el guardado de datos en medios de almacenamiento digitales.

Electricidad estática. Exceso de carga eléctrica en una zona de poca conductividad. Esta puede provocar cargas electrostáticas que son descargas de electricidad que se producen de forma repentina y que pueden provocar daños en los dispositivos electrónicos.

Esterilización. Aplicado a medios de almacenamiento de datos digitales, es el proceso de eliminación segura de la información almacenada previamente en un medio de almacenamiento digital, es decir, sin que queden rastros de información que haya sido almacenada previamente en el medio.

HASH. Función matemática que a través de la aplicación de un algoritmo permite obtener un código de longitud fija a partir de unos elementos de entrada de datos.

Imagen forense. Copia bit a bit de un medio de almacenamiento digital en la cual quedan grabados los datos tal y como se encuentran en el medio original.

Medios de almacenamiento. Medios físicos donde es posible almacenar los datos de sistemas computarizados y posteriormente leerlos o recuperarlos.

Microsoft Windows. Nombre de la familia de distribuciones de sistemas operativos para diversos dispositivos, desarrollados y distribuidos por Microsoft y que están disponibles para diversas arquitecturas.

Número de serie. Es un código alfanumérico que puede contener uno o más caracteres y que es asignado por un fabricante a un objeto con el fin de poder identificarlo y diferenciarlo de los demás objetos del mismo tipo.

Sistema Operativo. Término que se usa en informática para referirse al software que controla los procesos básicos de un computador y la interacción entre cada uno de sus componentes.

ANTECEDENTES

La norma ISO/IEC 27037:2012 indica que en los procesos de adquisición de evidencia es recomendable extraer dos copias verificadas, una principal y otra de trabajo. La copia principal no debería ser utilizada sino solamente para verificar el contenido de la copia de trabajo o para generar una nueva copia de trabajo en los casos en que esta se ve afectada por algún motivo.

La misma norma establece cuatro (4) pasos básicos para la extracción de elementos físicos de evidencia a partir de medios de almacenamiento apagados:

- Extraer los medios de almacenamiento del dispositivo si aún no han sido removidos.
- Preparar disco de destino donde va a ser almacenada la evidencia.
- Crear una imagen digital del disco original en el disco de destino utilizando para ello una herramienta de software adecuada.
- Sellar disco de destino.

Al considerar entre las muchas herramientas forenses existentes en el mercado para la extracción de imágenes de medios de almacenamiento se recomienda utilizar el software FTK Imager por tratarse de una herramienta bien conocida y utilizada a nivel mundial, que es de libre uso y de alta calidad técnica.

ALCANCE

Las actividades descritas en este instructivo deberán ser ejecutadas por miembros del Equipo de respuesta a incidentes de seguridad informática con el fin de adquirir elementos de evidencia a partir de dispositivos de almacenamiento de datos que están apagados y que

han sido extraídos del equipo de cómputo en el que se encontraban, en el caso de los discos duros internos.

DESCRIPCIÓN DE ACTIVIDADES

Antes de realizar este procedimiento es necesario:

- Disponer un medio de almacenamiento esterilizado donde almacenar la copia del original con el fin de evitar que la evidencia quede contaminada y pierda valor probatorio. Ver ***Instructivo para esterilización de medios de almacenamiento*.**

- Disponer de guantes de material aislante con los cuales manipular los medios de almacenamiento con el fin de evitar que estos puedan sufrir daño por una descarga accidental de electricidad estática.

- Disponer de un mecanismo de bloqueo contra escritura hardware o software antes de conectar el medio de almacenamiento al equipo de cómputo que se vaya a utilizar para realizar el procedimiento.

- Disponer de una libreta de notas donde llevar un registro de las actividades realizadas.

- Disponer de una superficie de material no conductor de electricidad donde poder manipular los medios de almacenamiento.

- Disponer de un equipo de cómputo con sistema operativo Windows donde esté instalado el software FTK Imager versión 3 o superior.

Una vez se ha verificado el cumplimiento de los pasos descritos anteriormente, y con el fin de mantener los principios de la informática forense en relación con la evidencia digital, cada uno de los pasos descritos a continuación debe ser registrado por el funcionario que realiza el procedimiento en la libreta de notas preparada para tal fin.

1. Registrar en la libreta de notas la hora de inicio del procedimiento, el nombre del funcionario que lo realiza y el número de caso si el procedimiento se realiza en respuesta a un caso iniciado por el grupo ERISI.

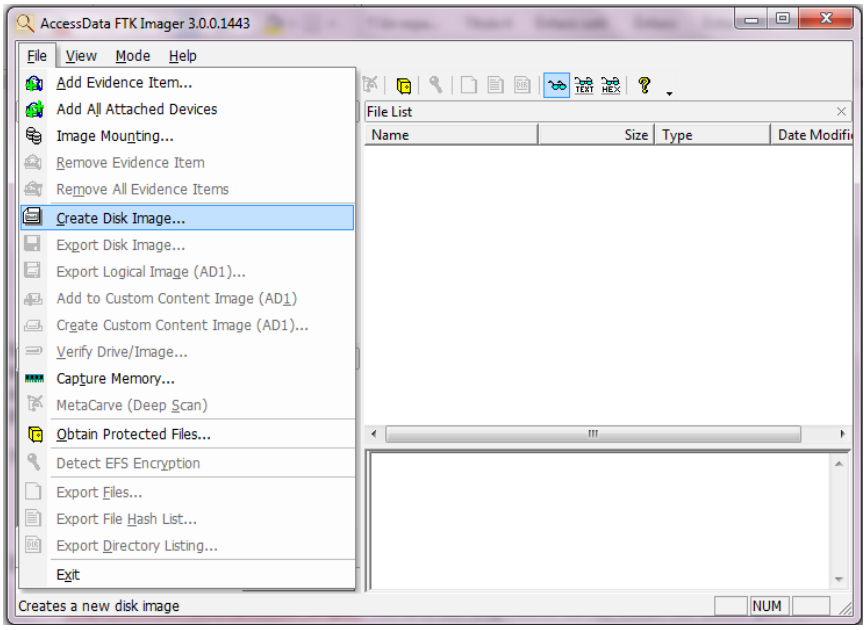
2. Si el medio dispositivo es recibido como parte de un caso forense y está bajo cadena de custodia, verificar que el medio de almacenamiento esté embalado en un contenedor etiquetado a prueba de descargas electrostáticas y que tanto el empaque como la etiqueta no muestren señales de adulteración.

3. Activar el mecanismo de bloqueo contra escritura y conectar el medio de almacenamiento del cual se va a extraer la imagen forense, teniendo en cuenta no pasar por alto el mecanismo de bloqueo contra escritura que se esté empleando.

4. Conectar un medio de almacenamiento esterilizado al equipo de cómputo con capacidad suficiente para almacenar la imagen forense que se vaya a extraer.

5. Abrir el aplicativo FTK Imager.

6. Una vez se abre la ventana de software, haga clic en el menú “File” y luego en “Create Disk Image…”.



7. En la ventana que se despliega seleccione el tipo imagen que desea extraer y haga clic en el botón siguiente. Para determinar cuál opción es la más adecuada, tenga en cuenta lo siguiente:

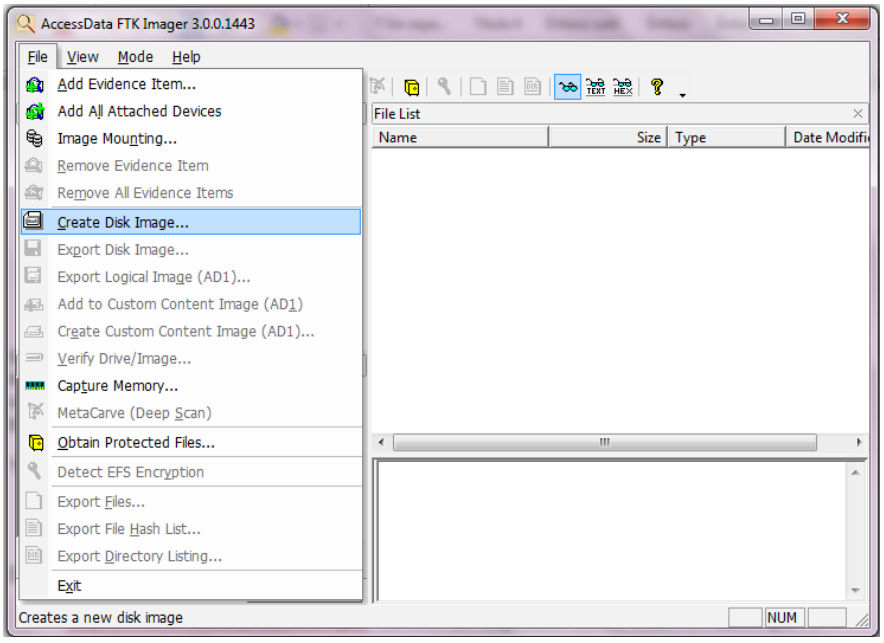
- Seleccione “Physical Drive” si quiere obtener una imagen bit a bit de todo el dispositivo. Para efectos del alcance de este instructivo, esta es la opción que deberá

ser seleccionada porque permite extraer una imagen bit a bit del contenido completo del medio de almacenamiento.

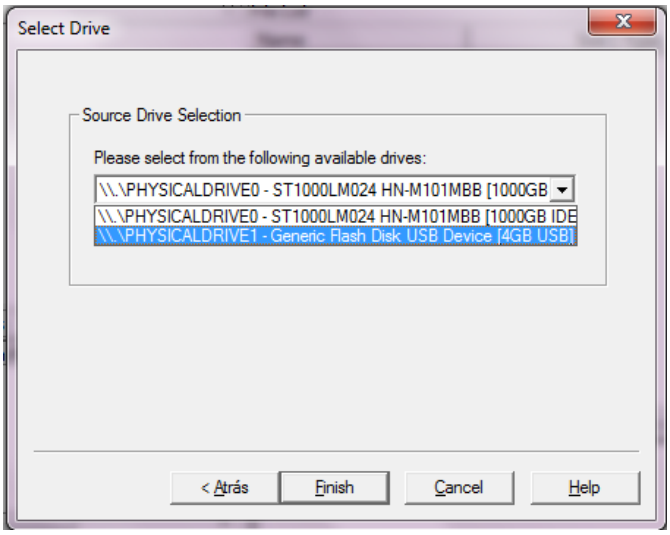
- Seleccione “Logical Drive” si quiere obtener una imagen de una unidad lógica instalada en el equipo.

- Seleccione “Image File” si desea extraer una imagen forense a partir de otra imagen existente.

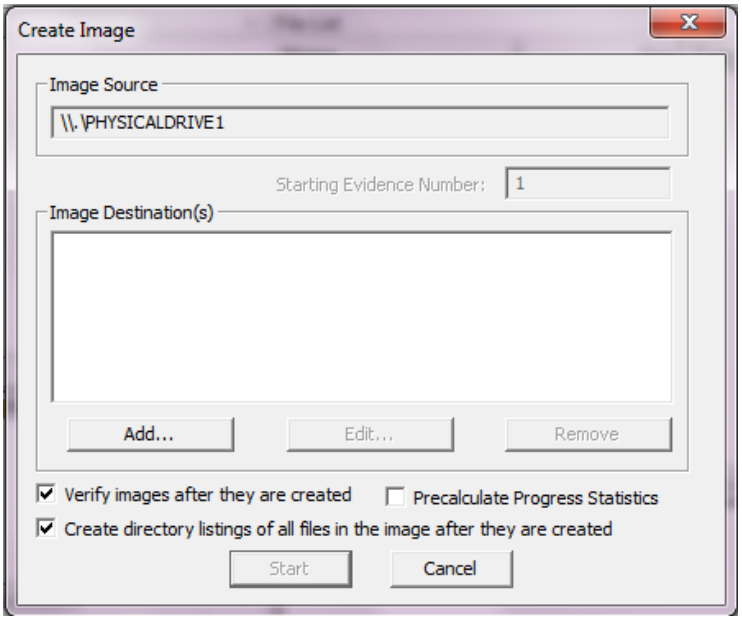
- Seleccione “Contents of a Folder” si desea extraer la imagen del contenido de una carpeta del sistema de archivos.



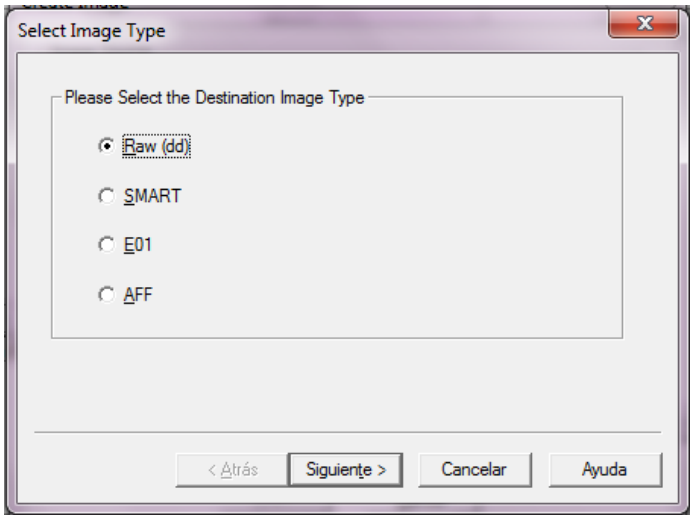
8. En el cuadro de diálogo que se muestra en pantalla, seleccione de la lista desplegable el dispositivo a partir del cual se va a extraer la imagen y haga clic en el botón “Finish”.



9. En el cuadro de diálogo que se despliega podrá indicar el tipo de imagen forense que se va a extraer y la ubicación donde se va a almacenar.

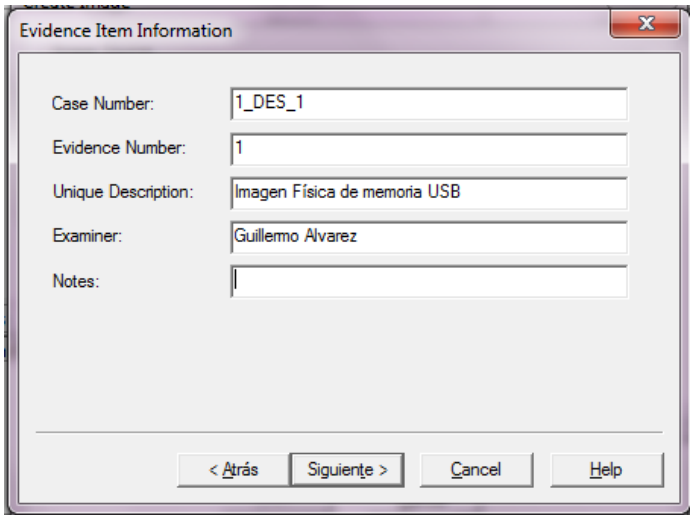


10. Al hacer clic en el botón “Add…”, el sistema despliega un cuadro de diálogo donde se debe seleccionar el formato que tendrá la imagen; seleccione el tercero de la lista (E01) y haga clic en el botón “Siguiente”.



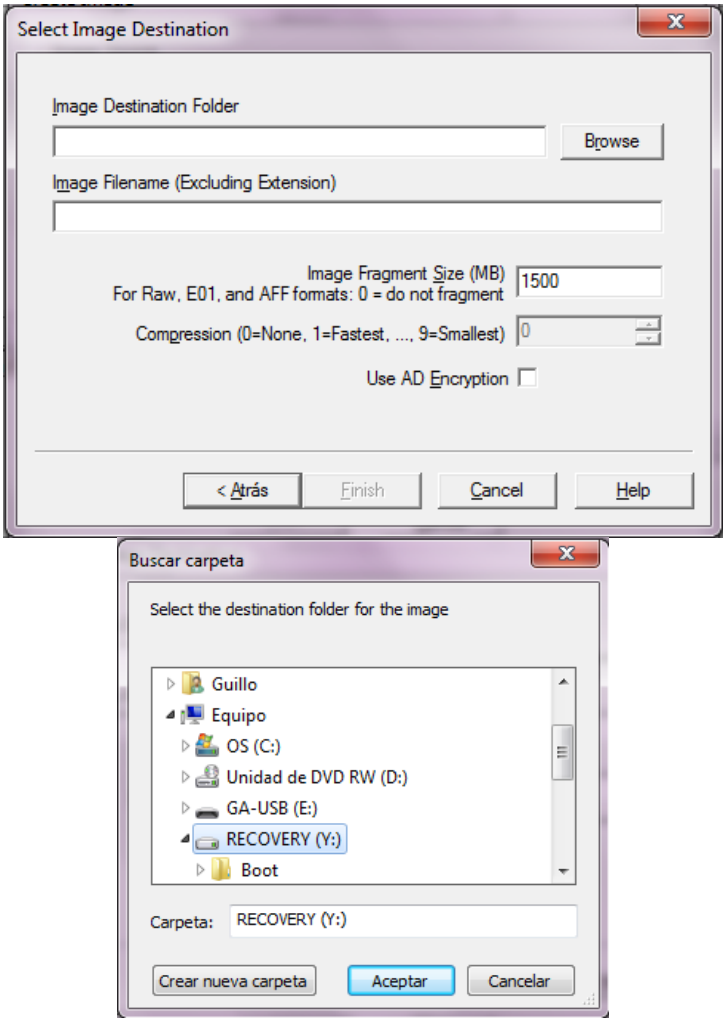
11. El sistema muestra un cuadro de diálogo donde es posible ingresar los datos del caso al cual corresponde la imagen forense. Los datos que se deben ingresar son:

- **Case Number.** Código asignado al caso de investigación iniciado en la organización.
- **Evidence Number.** Número consecutivo del elemento de evidencia asociado al caso.
- **Unique Description.** Descripción corta del elemento de evidencia.
- **Examiner.** Nombre del funcionario que extrae la imagen forense.
- **Notes.** Notas que sean relevantes en relación con la imagen forense.

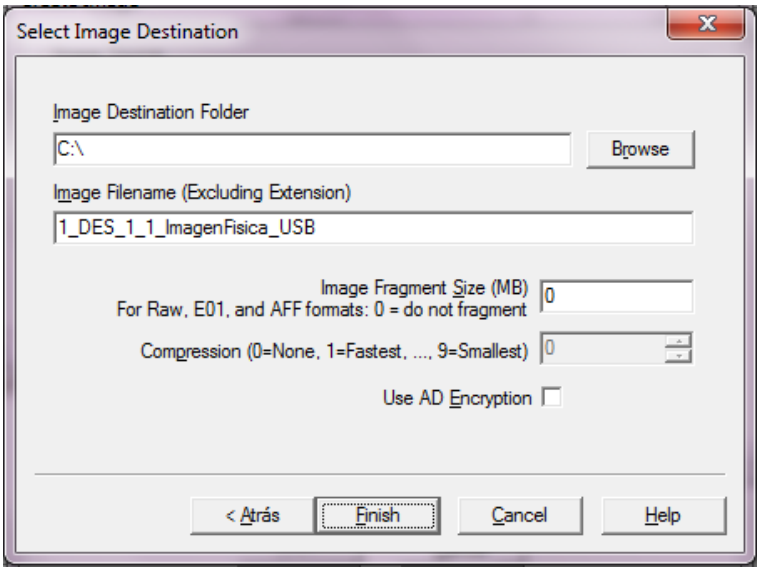


Una vez diligenciados estos campos haga clic en el botón “Siguiente”.

12. En el cuadro de diálogo que se despliega seleccione la ubicación donde se va a almacenar la imagen forense. Para ello haga clic en el botón “Browse” y en el cuadro de diálogo que aparece seleccione el medio de almacenamiento esterilizado y haga clic en el botón “Aceptar”.

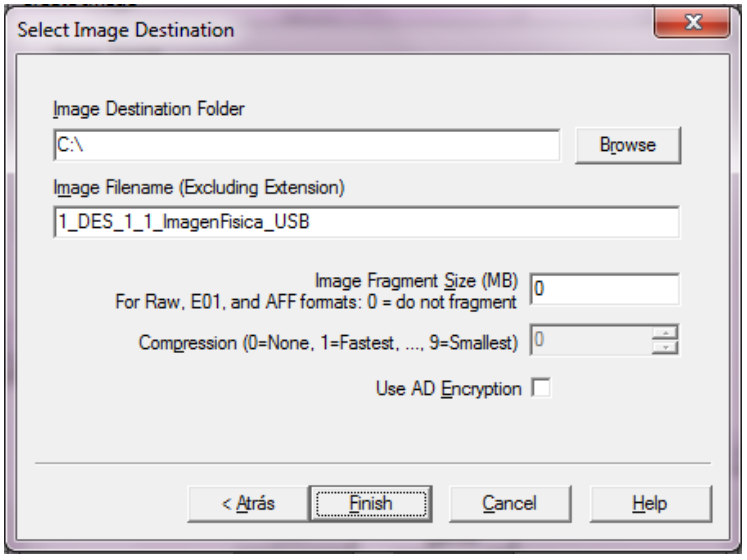


13. Diligencie el campo “Image Filename” utilizando el número del caso, el número de la evidencia y una breve descripción del medio como nombre de la imagen forense con el fin de ubicarla más fácilmente

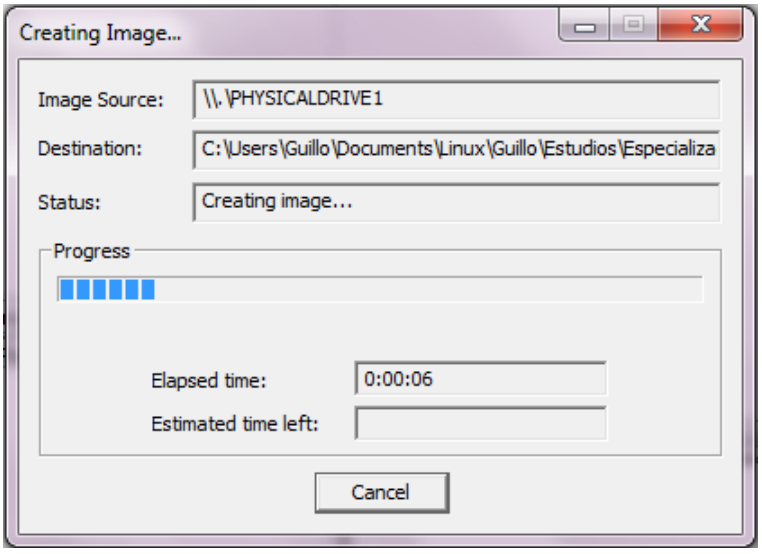


14. En el campo “Image Fragment Size” escriba 0, para no limitar el tamaño de la imagen que se va a extraer o un valor en Megabits con la capacidad del medio de almacenamiento cuando se va a partir la imagen y haga clic en el botón “Finish”.

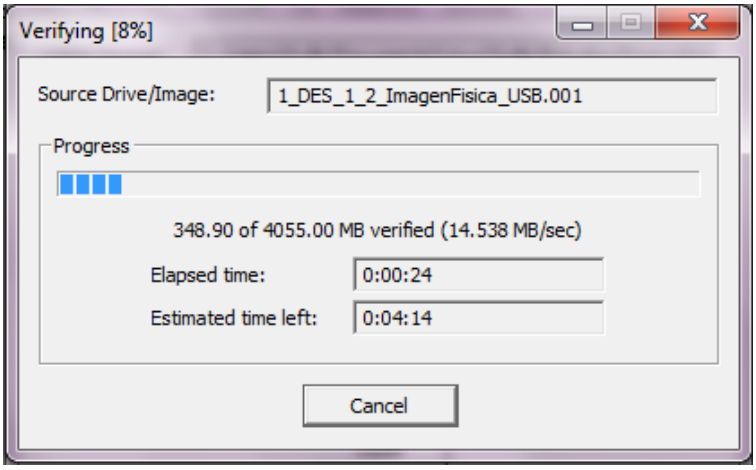
15. Una vez seleccionada la ubicación y el nombre de la imagen forense, el sistema muestra nuevamente la ventana de selección de la ubicación. Si por el tamaño de la imagen se requiere agregar más ubicaciones, asegúrese de tener conectados medios de almacenamiento esterilizados y repita los pasos 10 al 14 cuantas veces sea necesario. Al terminar haga clic en el botón “Finish”.



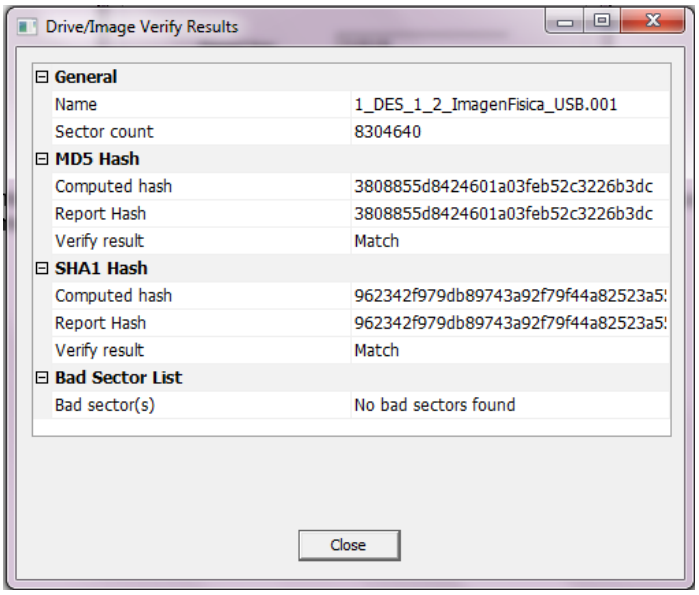
16. El sistema muestra un cuadro de diálogo donde es posible observar el avance del proceso de extracción de la imagen forense.



17. Terminado el proceso de extracción se inicia un proceso de verificación cuyo progreso es mostrado por el sistema en otro cuadro de diálogo.



18. Al finalizar el sistema muestra un resumen del procedimiento realizado indicando el nombre de la imagen, el tamaño en sectores del dispositivo, los códigos hash calculados a partir del contenido de la imagen y un informe de los errores encontrados en el medio de almacenamiento en caso que existan.



19. Verifique en el medio de almacenamiento seleccionado para almacenar la imagen forense que existan tres archivos así:

- Archivo(s) de imagen(es) forense(s) conforme a lo indicado en el paso 14. Este archivo(s) tiene como extensión un valor numérico de tres dígitos que indica el orden de las particiones que se generaron durante el proceso de extracción. Si se obtuvo un solo archivo de imagen la extensión siempre será 001.

- Un archivo con extensión csv con el mismo nombre de la imagen donde se enumeran cada uno de los archivos encontrados en la imagen forense.

- Un archivo con extensión txt con el mismo nombre de la imagen donde se almacena el reporte de las acciones realizadas por el aplicativo, incluyendo los códigos hash calculados.

Una vez finalizado el procedimiento, se deberá almacenar todos los dispositivos que contentan los archivos resultantes en una ubicación segura y ponerlos bajo cadena de custodia.

Elaborado por:	**Revisado por:**	**Aprobado por:**
GUILLERMO ÁLVAREZ Fecha: Noviembre de 2015		

Fuente: propio del autor

ANEXO H. INSTRUCTIVO PARA ESTERILIZACIÓN DE MEDIOS DE ALMACENAMIENTO

OBJETIVO

De acuerdo con las mejores prácticas de recolección de evidencia forense, con el fin de evitar que los datos recolectados sufran cualquier tipo de alteración que les haga perder valor probatorio, es necesario esterilizar los contenedores en los cuales se almacenan. Dada la naturaleza digital de la evidencia que se pretende proteger, los métodos de esterilización que se aplican a tales medios de almacenamiento deben tener la misma naturaleza y por lo tanto se deben utilizar herramientas adecuadas.

GLOSARIO

Disco duro. Término informático que hace referencia a dispositivos de almacenamiento de datos digitales de alta capacidad que pueden ser internos cuando están insertados de forma permanente en un computador o externos cuando pueden ser conectados o extraídos de un computador de acuerdo con la necesidad.

Esterilización. Aplicado a medios de almacenamiento de datos digitales, es el proceso de eliminación segura de la información almacenada previamente en un medio de almacenamiento digital, es decir, sin que queden rastros de información que haya sido almacenada previamente en el medio.

Mebibyte (MiB). Unidad de medida de información utilizada como un múltiplo del byte y que equivale a 2^{20} bytes.

Medios de Almacenamiento. Medios físicos donde es posible almacenar los datos de sistemas computarizados y posteriormente leerlos o recuperarlos.

Megabit (MB). Unidad de medida de información que equivale a 10^6 bits.

Número de serie. Es un código alfanumérico que puede contener uno o más caracteres y que es asignado por un fabricante a un objeto con el fin de poder identificarlo y diferenciarlo de los demás objetos del mismo tipo.

Sistema Operativo. Término que se usa en informática para referirse al software que

controla los procesos básicos de un computador y la interacción entre cada uno de sus componentes.

Software. Término que se usa en informática para referirse a un conjunto de sentencias o rutinas que indican a un computador qué hacer.

USB. Iniciales en inglés de Puerto Serial Universal (Universal Serial Bus) que es un puerto de comunicación estándar utilizado en múltiples dispositivos que se pueden comunicar con un computador.

GENERALIDADES

El manual de procedimientos del sistema de cadena de custodia generado por la Fiscalía General de la Nación, establece como uno de los factores críticos de éxito a tener en cuenta en los procesos de administración de evidencia, sin perder la trazabilidad de la cadena de custodia, la utilización de contenedores estériles, con el fin de asegurar y conservar las características de los elementos físicos de prueba. En el caso de los dispositivos de almacenamiento digital, la esterilización se logra eliminando de forma segura todos los datos que hayan sido almacenados previamente con el fin de evitar que los elementos de evidencia se vean contaminados y pierdan valor probatorio.

Existen diversas herramientas de software en el mercado que permiten realizar la eliminación segura de datos, tanto para sistema operativo Windows como para Linux. Ejemplos de herramientas en Windows son Eraser, DBAN, EnCase entre otros. El sistema operativo Linux por otra parte, provee herramientas nativas para el mismo fin tales como shred o wipe. Para efectos de la elaboración de este instructivo, se escogió EnCase, por tratarse de un software libre de uso y de alta calidad técnica.

ALCANCE

Las acciones que se describen en este instructivo deberán ser llevadas a cabo por miembros del grupo ERISI cuando se requiere llevar a cabo la eliminación segura de datos de dispositivos de almacenamiento. También puede ser utilizado por el personal del área de tecnología cuando se requiera eliminar todo rastro de información confidencial de los dispositivos de almacenamiento que han sido utilizados por la compañía.

DESCRIPCIÓN DE ACTIVIDADES

Para la ejecución de las actividades descritas a continuación, se debe disponer de un de ***Acta de esterilización de medios de almacenamiento***, donde se deberán registrar los datos correspondientes al medio y los resultados del proceso ejecutado.

1. Diligenciar el campo “Fecha Hora” con los datos correspondientes tomados al inicio del procedimiento. El formato de la fecha es el indicado en el acta como se describe a continuación: los primeros cuatro dígitos de la fecha corresponden al año (AAAA), los dos siguientes corresponden al mes (MM) y los dos últimos corresponden al día (DD), separados entre sí por una barra inclinada (/). A continuación se debe indicar la hora (hh) y el minuto (mm) en que se inició el procedimiento, así como el periodo horario (p) correspondiente (am ó pm).

2. Diligenciar con su nombre el campo “Nombre del funcionario”. Debe corresponder al nombre el funcionario que firma el documento y que por lo tanto asumirá la responsabilidad de su adecuada ejecución. Si el procedimiento es realizado con el fin utilizar el medio posteriormente para almacenamiento de evidencia forense, deberá ser un miembro del grupo ERISI quien lleve a cabo las actividades aquí descritas.

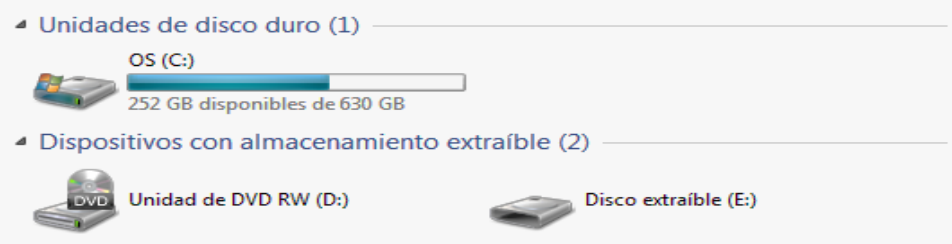
3. En el campo “Objetivo” del acta se debe indicar la razón por la que está realizando la eliminación segura de datos del dispositivo.

4. En el campo “Tipo de medio de almacenamiento” escriba el nombre genérico del dispositivo con el que es conocido en el mercado, por ejemplo: Memoria USB, disco duro interno, disco duro externo, etc.

5. En el campo “Serial” digite el número de serie del dispositivo que puede encontrar en las etiquetas adheridas al mismo y consta de una serie de caracteres alfanuméricos. Por lo general, cuando se incluyen caracteres alfabéticos en estos códigos, los fabricantes utilizan letras en mayúsculas. En el caso de los discos duros externos, este dato generalmente se puede encontrar buscando las siglas S/N o la palabra Serial. En el momento de diligenciar este dato en el formato, se debe tener especial cuidado de hacerlo con caracteres legibles evitando posibles ambigüedades como puede ocurrir al no saber diferenciar entre una letra ge mayúscula (G) y el número seis (6); o por confundir el número uno (1) de la vocal i en mayúscula (I) o la letra ele minúscula (l). Si no cuenta con esta información escriba en el campo la palabra “Desconocido”.

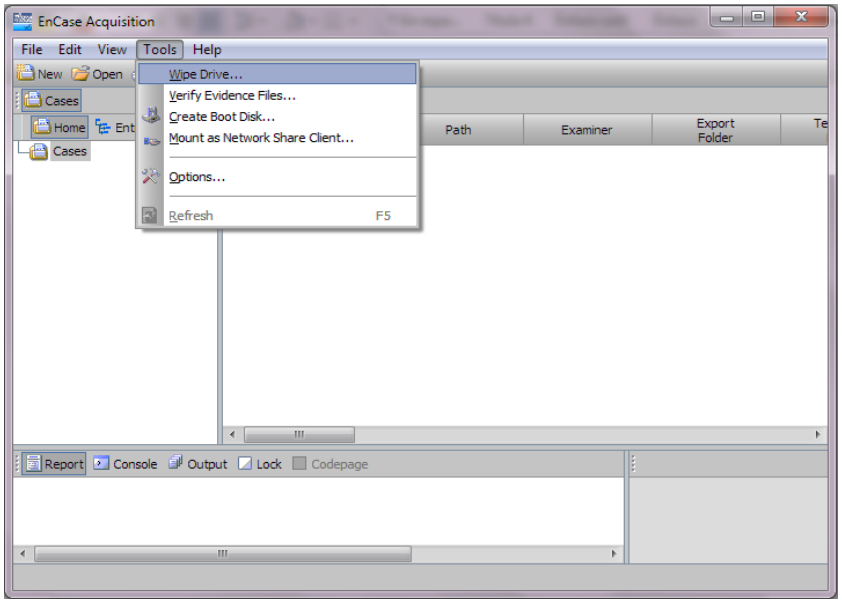
6. En el campo “Marca” digite la marca del dispositivo. Si no cuenta con esta información escriba en el campo la palabra “Desconocido”.

7. Conectar el medio de almacenamiento que desea esterilizar al equipo de cómputo e identificar en el navegador de Windows la unidad asignada por el sistema operativo. En la imagen de ejemplo, la unidad asignada es la letra E. Es importante en este punto identificar el dispositivo con plena certeza puesto que la eliminación de datos es irreversible y por lo tanto no se puede cometer el error de eliminar la información de un medio diferente, especialmente la del disco duro donde está alojado el sistema operativo del equipo de cómputo que se está utilizando.

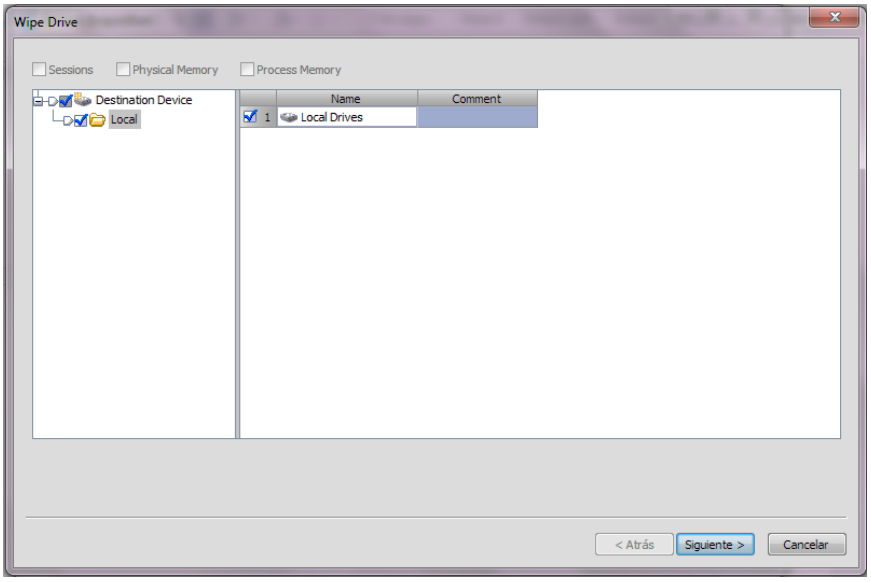


Una vez ha identificado la unidad, haga clic derecho sobre ella y luego clic en el menú Propiedades del menú que se despliega, para determinar la capacidad de almacenamiento de la unidad en GB, dato que permitirá más adelante encontrar la unidad en el software utilizado para la esterilización.

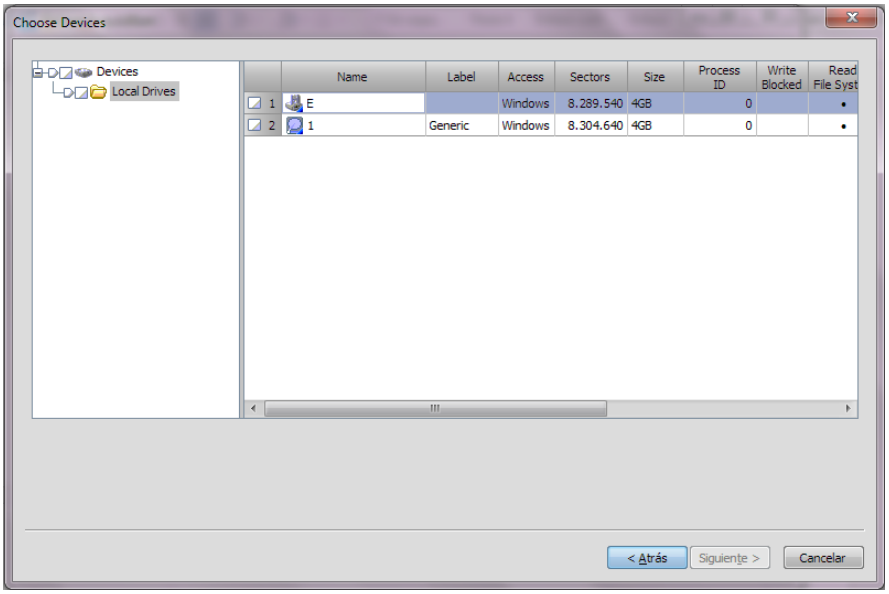
8. Abrir la herramienta de software EnCase y hacer clic en el menú Tools (Herramientas) y el submenú “Wipe Drive…”, que en castellano significa “Limpiar la unidad”, como se muestra en la imagen.



9. El software muestra una ventana donde aparecen las opciones disponibles en el sistema para seleccionar unidades, permitiendo seleccionar entre unidades locales, es decir, instaladas directamente en el equipo de cómputo, o remotas como es el caso de unidades de red. De la lista que se despliega seleccione la casilla del elemento “Local Drives” ubicado en la parte derecha de la ventana y haga clic en el botón “Siguiente”, ubicado en la parte baja de la ventana.



10. Se despliega una ventana donde se muestran las unidades físicas y lógicas instaladas en el sistema junto con información adicional sobre el medio en una tabla.



A continuación se describen los datos que se muestran en la tabla desplegada por medio de los cuales es posible identificar el dispositivo que se desea esterilizar

- **Name.** Nombre de la unidad física o lógica identificada conectada en el sistema. En el caso de la unidad lógica, se mostrará el literal asignado al dispositivo que corresponde con el identificado en el paso siete (7) en el explorador de Windows. En el caso de las imágenes de ejemplo es la letra E.

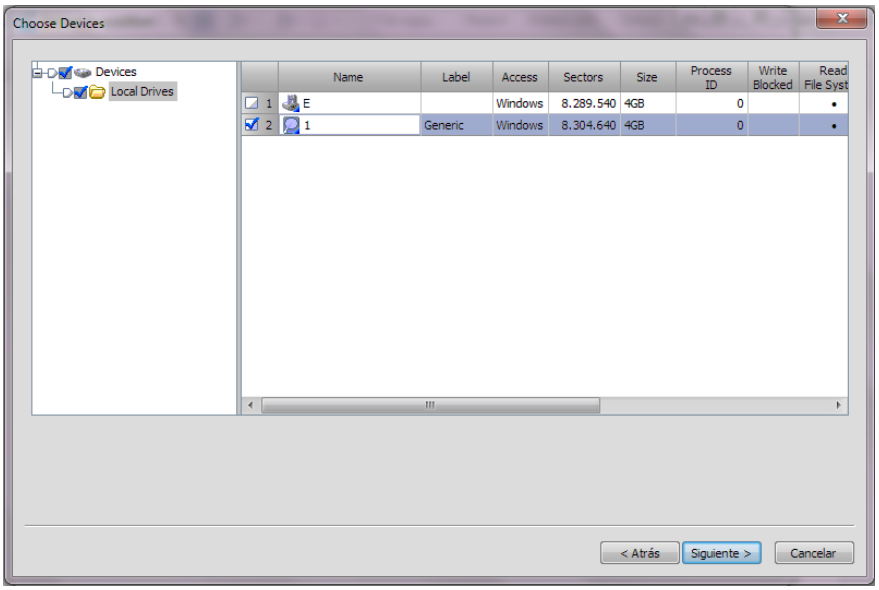
- **Label.** Etiqueta con que la unidad fue nombrada. En el caso de la unidad lógica, se mostrará el mismo nombre de etiqueta que aparece en el explorador de Windows. Cuando una etiqueta no ha sido asignada, este campo aparece vacío. En las unidades físicas, en este campo se muestra el nombre asignado por el fabricante que en el caso de la imagen de ejemplo es Generic.

- **Sectors.** Número de sectores que tiene el dispositivo. Con este dato es posible identificar cuál unidad física corresponde a la unidad lógica ya identificada por medio del nombre y etiqueta de la unidad.

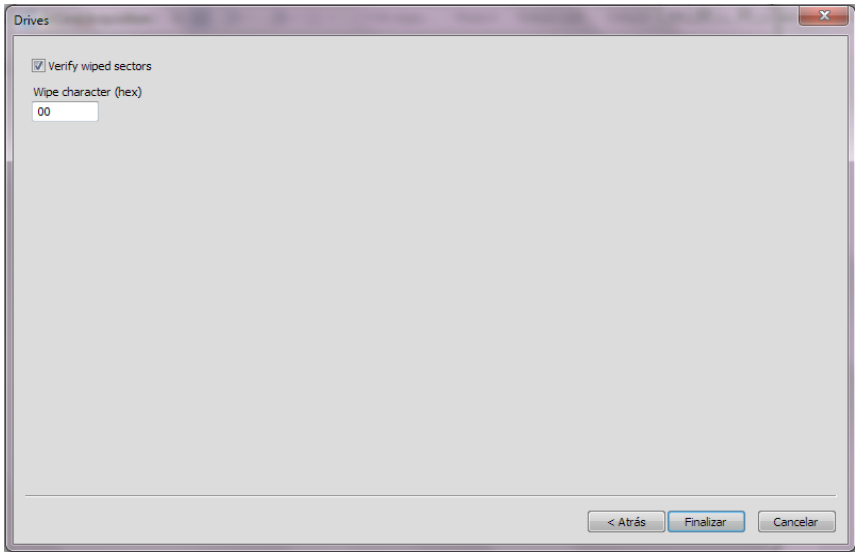
- **Size.** Capacidad de almacenamiento de datos en GB. Debe corresponder con la capacidad del dispositivo identificada al final del punto siete (7) de este instructivo.

11. Diligenciar en el acta, en el campo “Capacidad total de almacenamiento”, el número indicado en la columna “Size” que muestra el software y la unidad de medida GB.

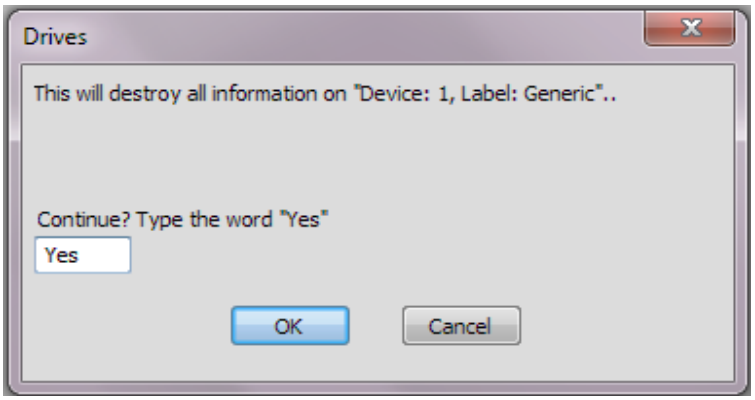
12. Ubicar la unidad física correspondiente al medio que se va a esterilizar. Las unidades físicas son las que están marcadas con el icono de un disco y una aguja como se observa en la imagen a continuación. Para identificar la unidad adecuada, seleccione aquella cuyos datos en los campos Size y Sectors corresponde con la que tiene el literal del medio que se ubicó anteriormente. Seleccione la casilla de selección que aparece al inicio del registro correspondiente y haga clic en el botón “Siguiente”.



13. En la ventana que se muestra, seleccione la casilla de selección marcada con la etiqueta “Verify speed sectors” y digite el valor hexadecimal que va a ser asignado a cada espacio de almacenamiento en el medio. Deje el valor que el software asigna por defecto (00) y haga clic en el botón Finalizar.

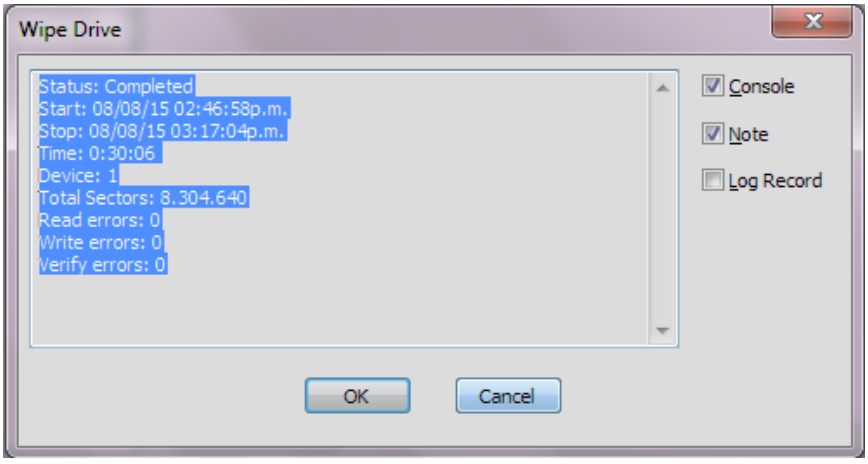


14. Dado que el proceso que se va a iniciar es irreversible y que los datos almacenados en el medio van a ser irrecuperables, el software solicita confirmación a través de la ventana que se despliega. Para confirmar y continuar con el proceso, en el campo de texto que se muestra bajo la leyenda “Continue? Type the Word ‘Yes’”, digite la palabra “Yes” y haga clic en el botón “OK”.



15. En la esquina inferior derecha de la ventana principal del aplicativo se muestra el progreso del proceso. El primer paso ejecutado por la herramienta es el borrado seguro de los datos (wipe). Una vez terminado, se da inicio automáticamente el segundo paso que es la verificación (verifying). Este proceso puede tomar varios minutos dependiendo del tamaño de la unidad.

16. Al finalizar, la herramienta muestra un resumen del procedimiento con los resultados obtenidos. Diligencie esta información en el acta e esterilización, en el campo "Reporte generado por la herramienta" antes de hacer clic en el botón "OK".



17. Si en el reporte que muestra la herramienta se encuentran valores diferentes a 0 en las líneas "Read errors", "Write errors" o "Verify error", diligencie los tres datos mencionados en la sección "Reporte de fallos" del acta con el fin de dejar constancia de los fallos que la herramienta detectó y corrigió (o no pudo corregir) en el medio de almacenamiento.

18. Si el acta diligenciada está en formato impreso, se debe firmar el documento y almacenarlo en un lugar seguro. Si se trata de un documento digital se debe almacenar en un repositorio documental utilizando las credenciales de acceso del funcionario que realizó el procedimiento o ser enviado a una cuenta de correo electrónico de tal manera que quede constancia de quién llevó a cabo el procedimiento y de los resultados del mismo.

Una vez terminado el proceso de eliminación segura, de manera opcional se recomienda dar formato al disco para que pueda ser utilizado para el grabar datos, especialmente si el motivo de la ejecución del instructivo no es el almacenamiento de imágenes forenses.

Elaborado por:	**Revisado por:**	**Aprobado por:**
GUILLERMO ÁLVAREZ Fecha: Noviembre de 2015		

Fuente: propio del autor.

ANEXO I. INSTRUCTIVO PARA RECOLECCIÓN DE DATOS VOLÁTILES

OBJETIVO

Este procedimiento está orientado a la recolección de los datos volátiles de un equipo de cómputo que funciona con sistema operativo Windows XP, Windows Vista, Windows 7 y/o Windows 8.

GLOSARIO

Bitácora: Medio escrito donde se registran anotaciones que se consideran útiles para el seguimiento de una serie de eventos.

Datos volátiles: Datos que pueden contener evidencia forense que están almacenados en los medios de memoria volátil de un equipo de cómputo tal como la memoria RAM los cuales se pierden en el momento de interrumpirse el flujo eléctrico.

Dirección MAC: Siglas en inglés de Media Access Control que es un identificador único asignado por el fabricante para una tarjeta o dispositivo de red. Es conocida también como dirección física.

Evidencia forense. Todo indicio que permite establecer a través de métodos científicos, una relación entre un crimen y quien lo cometió.

Medios de almacenamiento. Medios físicos donde es posible almacenar los datos de sistemas computarizados y posteriormente leerlos o recuperarlos.

Microsoft Windows. Nombre de la familia de distribuciones de sistemas operativos para diversos dispositivos, desarrollados y distribuidos por Microsoft y que están disponibles para diversas arquitecturas.

RAM: Sigla de Random Access Memory o memoria de acceso aleatorio que es el espacio de almacenamiento de datos temporal de una computadora y donde se alojan los datos que permiten operaciones de lectura y escritura.

Sistema Operativo. Término que se usa en informática para referirse al software que controla los procesos básicos de un computador y la interacción entre cada uno de sus componentes.

Software. Término que se usa en informática para referirse a un conjunto de sentencias o rutinas que indican a un computador qué hacer.

DESCRIPCIÓN DE ACTIVIDADES

PREPARACIÓN

Antes de comenzar se deberán realizar las siguientes verificaciones:

1. El equipo de cómputo está encendido y conectado a una red eléctrica constante. Esto con el fin de evitar que el equipo de cómputo se apague antes de terminar.

2. Se cuenta con un medio de almacenamiento externo previamente esterilizado. Ver ***Instructivo para esterilización de medios de almacenamiento***.

3. En el medio de almacenamiento se encuentran los siguientes elementos de software :
   - date.exe
   - netstat .exe
   - pslist.exe
   - systeminfo.exe
   - listdlls.exe
   - psservice.exe
   - psloglis.exe
   - psloggedon.exe
   - arp.exe
   - ipconfig.exe
   - dir.exe

   Todos estos archivos ejecutables están almacenados en la carpeta sw.

4. En el medio de almacenamiento se encuentra el archivo ExtraerEvidencia.bat que permite automatizar la ejecución de los comandos correspondientes a los elementos de software descritos en el punto anterior con el fin de agilizar y asegurar la adecuada extracción de los datos volátiles.

5. Contar con un cuadernillo de notas.

EJECUCIÓN

Los datos volátiles pueden contener evidencia relevante para análisis forenses posteriores y la utilidad de dicha información dependerá en gran medida de la rigurosidad con que el procedimiento se lleve a cabo. Por tal razón, en caso de no poder realizar alguno de los pasos descritos a continuación, en la bitácora llevada por el investigador debe quedar constancia explícita del motivo de la omisión. Para todos los comandos indicados en los pasos siguientes se debe anotar en la bitácora la hora y minuto de ejecución y el nombre del comando ejecutado.

1. Anotar la fecha y hora del inicio del procedimiento así como el número del caso que se está atendiendo el cual deberá corresponder con el número registrado en la bitácora de incidentes de seguridad y que deberá estar asociado al incidente que dio inicio al caso. El formato de fecha y hora será de cuatro dígitos numéricos para el año, dos dígitos numéricos para el mes y dos dígitos numéricos para el día y deberá incluir la hora (hh) y el minuto (mm) en que se inició el procedimiento, así como el periodo horario (p) correspondiente (am ó pm).

2. Anotar el nombre del funcionario que realiza el procedimiento. Deberá corresponder con el nombre de uno de los miembros del grupo ERISI quien asumirá la responsabilidad de la correcta ejecución de cada una de las acciones contenidas en este instructivo.

3. Anotar el nombre del funcionario a quien se ha asignado el equipo de cómputo objeto de investigación y el área de la compañía donde el equipo está ubicado.

4. Indicar brevemente el motivo del procedimiento. En este punto se deberán indicar motivaciones legales o procedimentales que pueden ser de la empresa o de acuerdo con normas nacionales o internacionales que avalen la necesidad de adelantar las actividades descritas en este instructivo.

5. Insertar el medio de almacenamiento donde se encuentra el software que permitirá la extracción de los datos volátiles. En este punto se deberá identificar la unidad asignada al medio de almacenamiento por el sistema operativo con el fin de utilizarlo en el punto siguiente.

6. Haciendo uso del explorador de Windows, ubicarse en la unidad asignada por el sistema operativo al medio de almacenamiento donde está el software de extracción y en la carpeta donde está almacenado el archivo ExtraerEvidencia.bat.

7. Hacer doble clic en el archivo ExtraerEvidencia.bat. Se abre una ventana que proporciona una consola de línea de comandos (CMD) donde se pregunta el literal asignado por el sistema operativo al medio de almacenamiento donde se encuentran los elementos de software que van a permitir la extracción de la evidencia, que es también el dispositivo donde dicha evidencia va a ser almacenada. Digite el dato solicitado y presione la tecla Enter.

8. En la ventana donde está la consola de línea de comandos (CMD) se solicita el nombre de la carpeta donde van a quedar guardados los elementos de evidencia. Digite la palabra Evidencia y oprima la techa Enter.

9. El archivo .bat contiene las sentencias necesarias para ejecutar la extracción de la evidencia volátil del sistema y almacenarla en el medio de almacenamiento que se esté utilizando. En algunos casos, se mostrará en pantalla una ventana donde se solicita la aceptación de los términos y condiciones de uso de los elementos de software utilizados. Para continuar con el procedimiento simplemente haga clic en el botón aceptar de las ventanas emergentes hasta que en la ventana donde está la consola de línea de comandos aparezca el mensaje “Procedimiento terminado satisfactoriamente”.

10. Usando el explorador de Windows ingrese a la recién creada carpeta Evidencia y verifique que se encuentren almacenados los siguientes archivos:

    - date.txt
    - netstat.txt
    - pslist.txt
    - systeminfo.txt
    - listdlls.txt
    - psservice.txt
    - psloglist.txt
    - psloggedon.txt
    - arp.txt
    - ipconfig.txt
    - dir.txt

11. Si alguno de los archivos no se encuentra, ejecute el comando correspondiente al archivo que faltante siguiendo uno de los pasos que se describen a continuación. En la ejecución de los comandos se sigue la estructura que se define a continuación: <nombre del comando> /<opciones> <ruta donde se van a guardar los archivos>, que para efectos de este instructivo es la carpeta Evidencia y finalmente <nombre

del comando>.txt que corresponde con el nombre del elemento de evidencia recolectado. Si todos los archivos fueron creados correctamente, pase al punto 3 de este instructivo.

12. Ejecutar el comando date /t > ../Evidencia/date.txt para tomar la fecha del sistema con el fin de determinar si la fecha del sistema ha sido alterada y no corresponde con la fecha real.

13. Ejecutar el comando time /t > ../Evidencia/time.txt para tomar la hora del sistema con el fin de determinar si la hora del sistema ha sido alterada y no corresponde con la hora real.

14. Ejecutar el comando netstat -an > ../Evidencia/netstat.txt el cual permite visualizar la lista de puertos en uso con la siguiente información:
    - Puerto
    - IP Origen
    - IP Destino
    - Estado del puerto

15. Ejecutar el comando pslist > ../Evidencia/pslist.txt, sin parámetros con el fin de consultar los procesos que se encuentran en ejecución en el momento de la intervención.

16. Ejecutar el comando systeminfo > ../Evidencia/systeminfo.txt, sin parámetros con el fin de conocer los datos propios del sistema operativo y la configuración del sistema.

17. Ejecutar el comando listdlls > .. listdlls.txt el cual muestra todas las librerías que están en uso en el momento de la intervención. Este paso es importante puesto que eventualmente puede permitir asociar una dll con un software malicioso en un momento dado.

18. Ejecutar el comando psservice > ../Evidencia/psservice.txt el cual muestra todos los servicios que están activos.

19. Ejecutar el comando psloglist > ../Evidencia/psloglist.txt el cual muestra todas las auditorías encendidas y el momento de su inicio. Esta información es particularmente útil si el equipo de cómputo tiene activada la opción de congelación de disco, la cual elimina todos los cambios realizados en el sistema una vez se apaga el equipo de cómputo.

20. Ejecutar el comando psloggedon > ../Evidencia/psloggedon.txt el cual muestra los usuarios que tengan una sesión iniciada en el sistema y que están activos.

21. Ejecutar el comando arp -a > ../Evidencia/arp.txt el cual muestra las direcciones MAC de todas las conexiones de red existentes.

22. Ejecutar el comando ipconfig /all > ../Evidencia/ipconfig.txt el cual permite conocer todas las interfaces de red existentes en el sistema.

23. Indicar en la bitácora la hora de culminación del procedimiento.

Una vez terminados los pasos descritos, se deberá poner el medio de almacenamiento que se utilizó para realizar el procedimiento en cadena de custodia.

Elaborado por:	**Revisado por:**	**Aprobado por:**
GUILLERMO ÁLVAREZ Fecha: Noviembre de 2015		

Fuente propia del autor.

ANEXO J. INSTRUCTIVO PARA RECOLECTAR MEDIOS DE ALMACENAMIENTO DE DATOS

OBJETIVO

Este instructivo se deberá ejecutar cuando se quiere hacer un inventario de medios de almacenamiento de datos en formato digital que van a ser puestos bajo cadena de custodia para ser utilizados en un proceso de investigación de informática forense.

GLOSARIO

Bit. Acrónimo de dígito binario. Corresponde a la unidad mínima de almacenamiento de datos binarios utilizados en informática y en cualquier dispositivo digital.

Medios de almacenamiento. Medios físicos donde es posible almacenar los datos de sistemas computarizados y posteriormente leerlos o recuperarlos.

Electricidad estática. Exceso de carga eléctrica en una zona de poca conductividad. Esta puede provocar cargas electrostáticas que son descargas de electricidad que se producen de forma repentina y que pueden provocar daños en los dispositivos electrónicos.

Mebibyte (MiB). Unidad de medida de información utilizada como un múltiplo del byte y que equivale a 2^{20} bytes.

Megabit (MB). Unidad de medida de información que equivale a 10^6 bits.

Número de serie. Es un código alfanumérico que puede contener uno o más caracteres y que es asignado por un fabricante a un objeto con el fin de poder identificarlo y diferenciarlo de los demás objetos del mismo tipo.

Tarjeta controladora. La tarjeta controladora es la parte encargada de gestionar la energía, mantener la rotación y el movimiento de diferentes partes del disco en niveles operativos, hace la corrección de errores, y controla el flujo de datos que entran y salen de los platos magnéticos donde se almacena la información: Básicamente es el cerebro del disco duro.

USB. Iniciales en inglés de Puerto Serial Universal (Universal Serial Bus) que es un puerto de comunicación estándar utilizado en múltiples dispositivos que se pueden comunicar con un computador.

ANTECEDENTES

Los medios de almacenamiento se han transformado con el paso del tiempo a la par de los avances tecnológicos, y en la actualidad, si bien los discos rígidos siguen dominando el mercado, existen varios tipos de medios como los que se mencionan a continuación, incluyendo algunos ejemplos:

- **Medios magnéticos:** discos duros rígidos, cintas magnéticas.
- **Medios ópticos:** CD-ROM, CD-R, CD-RW, DVD ± R, DVD ± RW.
- **Medios electrónicos:** memorias Flash, (llaveros) USB, SmartMedia, CompactFlash, discos SSD (discos de estado sólido).

DESCRIPCIÓN DE ACTIVIDADES

1. El funcionario que realiza el procedimiento deberá diligenciar en el Formato de Inventario de Medios de almacenamiento los datos de la sección "Información General" así:

   - **Fecha y hora en que se realiza el procedimiento.** El formato de la fecha es el indicado en el formato como se describe a continuación: los primeros cuatro dígitos de la fecha corresponden al año (AAAA), los dos siguientes corresponden al mes (MM) y los dos últimos corresponden al día (DD), separados entre sí por una barra inclinada (/). A continuación se debe indicar la hora (HH) y el minuto (MM) en que se inició el procedimiento, así como el periodo horario correspondiente (am ó pm).
   - **Nombre completo del funcionario que realiza el procedimiento.**, así como los datos del responsable del equipo: nombre, cargo y área.

2. Se deben diligenciar en el mismo formato, en la sección "Datos del responsable del dispositivo", los datos del funcionario bajo cuya responsabilidad están los medios de almacenamiento así:

   - Nombres y apellidos del funcionario. Si no es posible identificar al funcionario en el momento en que se realiza la diligencia, se deberá tomar este dato del inventario de la compañía.
   - Cargo que desempeña el funcionario dentro de la empresa.

- Área de la compañía a la que pertenece el funcionario.

3. Si los medios de almacenamiento hacen parte de un equipo de cómputo, como en el caso de los discos duros internos, se debe indicar su número de serie o el código de inventario interno asignado por la organización. En caso de no contar con esta información, se deberá obtener del registro de inventario de la compañía. Si el equipo no está registrado en el inventario, se deberá etiquetar al equipo durante el procedimiento con un número de identificación único para el caso, anotando este número en el formato de inventario e indicando en una bitácora de forma detallada los pasos realizados para la identificación y al finalizar poner todo el equipo en cadena de custodia.

4. Antes de manipular el dispositivo, se debe asegurar que no tenga fluido eléctrico circulando durante el proceso de recolección. Por ejemplo, en el caso de los discos duros internos, el equipo de cómputo debe estar apagado y desconectado de cualquier fuente eléctrica, incluyendo la batería extraíble en el caso de los equipos portátiles.

5. El funcionario que realiza el procedimiento debe proteger sus manos con guantes de materiales no conductores de electricidad para eliminar la posibilidad de una descarga de electricidad estática que eventualmente puede ocasionar daños en los dispositivos, por ejemplo en la tarjeta controladora de los discos duros.

6. Durante todo el procedimiento, asegurarse de colocar los dispositivos en una superficie no conductora de electricidad para evitar daño accidental por descarga eléctrica.

7. Diligenciar en el formato la sección “Datos del dispositivo” así:

    - **Tipo de medio de almacenamiento.** Tener en cuenta los tipos de medios de almacenamiento mencionados en los antecedentes de este documento. Indicar tanto la clasificación como el nombre del medio. Por ejemplo: Medio magnético / Disco duro.

    - **Número serial.** Código que permite identificar de forma unívoca el dispositivo. De no contar con el número serial como sucede con las memorias USB, se deberá etiquetar y asignar un número único que será utilizado también en el caso de investigación forense.

    - **Marca.** Nombre de la marca creada por el fabricante.

    - **Capacidad de almacenamiento.** Número de bits que el dispositivo es capaz de almacenar. Se debe indicar si el valor diligenciado en el formato está en Megabits o en Mebibytes.

Una vez cumplidos los pasos descritos anteriormente, se deberá entregar los elementos recolectados al área encargada del almacenamiento de evidencia forense.

Elaborado por:	**Revisado por:**	**Aprobado por:**
GUILLERMO ÁLVAREZ Fecha: Noviembre de 2015		

Fuente: propio del autor.

ANEXO K. INSTRUCTIVO PARA REPORTE DE INCIDENTES DE SEGURIDAD

OBJETIVO

Por medio de este instructivo se sientan las bases para el diligenciamiento del formato de reporte de incidentes de seguridad de la información de manera ordenada y detallada con el fin de asegurar que los funcionarios que realicen la gestión de reporte de un incidente, lo hagan de acuerdo a las políticas de la empresa y de manera estándar según lo establecido en el sistema de gestión de incidentes definido por PTESA.

GLOSARIO

Bitácora: Medio escrito donde se registran anotaciones que se consideran útiles para el seguimiento de una serie de eventos.

ERISI. Siglas de Equipo de Respuesta a Incidentes de Seguridad Informática. Se refiere al grupo de personas dentro de la empresa encargado de evaluar, documentar y gestionar los incidentes de seguridad informática.

Incidente de Seguridad Informática. Cualquier hecho que afecta o podría afectar la seguridad informática de la organización.

Ingeniería social. Técnica utilizada para obtener información confidencial a través de la manipulación de usuarios legítimos.

Malware. Término informático que se refiere a todo elemento de software malintencionado elaborado con el fin de infiltrarse, dañar o modificar sistemas de información sin el consentimiento del propietario.

Phishing. Es un término informático que califica un modelo de abuso informático y que se comete mediante el uso de un tipo de ingeniería social caracterizado por intentar adquirir información confidencial de forma fraudulenta

PTESA. Acrónimo de Profesionales en Transacciones Electrónicas. Nombre de la empresa tomada como base para la realización del trabajo de grado.

Seguridad de la Información. Conjunto de normas preventivas y reactivas que se toman frente a los sistemas de información de una organización con el fin de resguardar y proteger las características de la información: integridad, confidencialidad y disponibilidad.

Software. Término que se usa en informática para referirse a un conjunto de sentencias o rutinas que indican a un computador qué hacer.

Vulnerabilidad. Debilidad de un sistema informático que puede ser aprovechada por una amenaza para causar daños o alteraciones en el sistema.

GENERALIDADES

De acuerdo con la Guía Técnica Colombiana 169, es necesario "concientizar a todo el personal de la organización a través de instrucción y/u otros mecanismos, sobre la existencia del sistema de gestión de incidentes, sus beneficios y la manera de reportar un evento de seguridad de la información. Se recomienda suministrar entrenamiento adecuado al personal responsable de administrar el sistema de gestión de incidentes de seguridad de la información, a los que determinan si los eventos de seguridad de la información son incidentes, y a los involucrados en la investigación de los incidentes".

ALCANCE

Este procedimiento está dirigido a los miembros del ERISI, quienes por las políticas de seguridad de la información de la empresa, son el conducto regular para el reporte de incidentes de seguridad y por lo tanto, son los llamados a conocer al detalle la manera de documentar adecuadamente los eventos reportados o identificados.

DESCRIPCIÓN DE ACTIVIDADES

Cuando uno de los miembros del ERISI recibe o identifica un evento de seguridad y determina que es un incidente, procederá a reportarlo primero en la bitácora de incidentes – ver ***Instructivo para diligenciar bitácora de incidentes de seguridad*** - y posteriormente levantará el registro del incidente mismo utilizando el ***Formato para reporte de incidentes de seguridad de seguridad informática*** cuyos campos se describen a continuación.

- **Fecha y hora en que se diligenció el reporte.** Corresponde con la fecha y hora reportada en la bitácora de incidentes incluyendo año, mes, día, hora, minuto y periodo horario (a.m. ó p.m.).

- **Funcionario que diligencia el formato.** Nombre completo del miembro del grupo ERISI que recibe el reporte y procede a diligenciar los datos del mismo.

DATOS PERSONALES

Los datos a los que hace referencia esta sección corresponden a la persona que identificó el incidente y lo comunicó al ERISI.

- **Nombre completo.** Nombre y apellidos del funcionario.

- **Cargo.** Cargo asignado al funcionario dentro de la empresa.

- **Área.** Área o división de la empresa donde labora el funcionario.

- **Correo electrónico.** Dirección de correo electrónico de contacto del funcionario. Debe asegurarse de diligenciar aquí la cuenta de correo institucional, no la de uso personal.

- **Teléfono interno.** Número de teléfono de contacto del funcionario al interior de la empresa. Se debe incluir el número de extensión si aplica.

- **Teléfono particular.** Número de teléfono de contacto donde ubicar al funcionario fuera de las instalaciones de la empresa.

INFORMACIÓN SOBRE EL INCIDENTE

En esta sección se registran los datos relacionados con el incidente de seguridad tales como su clasificación, descripción, modo de detección y duración.

- **Fecha y hora en que se suscitó el incidente.** Diferente a la fecha en que el incidente fue reportado. Corresponde a la ubicación en el tiempo de la ocurrencia de los hechos que dieron lugar al incidente de seguridad.

- **Clasificación.** En esta sección es posible determinar el tipo de incidente que se reporta con base en las acciones más comunes que dan lugar a un reporte de seguridad. Para un mismo incidente es posible identificar uno o más de los elementos que se describen a continuación.

- **Uso indebido de información.** Cuando se evidencia que personal interno o externo no autorizado utiliza información que puede o no ser de propiedad la empresa sin el debido consentimiento del propietario.

- **Cambio en la configuración de un equipo.** Cuando sin mediar autorización explícita del administrador de un equipo, se realizan cambios en la configuración del mismo, sea que estos cambios afecten o no el funcionamiento del equipo.

- **Uso inadecuado de recursos informáticos.** Cuando un funcionario de la empresa o un tercero bajo cuya tutela la empresa haya entregado un equipo, sistema o herramienta informática, hace uso del elemento recibido por fuera de los términos establecidos por la compañía.

- **Ataque o infección de malware, o código malicioso (virus, gusanos, troyanos, etc.).** Incluye cualquier tipo de infección ataque por medio de software mal intencionado identificado en sistemas, documentos y/o dispositivos bajo responsabilidad de la empresa o propiedad privada de empleados o terceros a quienes se les haya concedido acceso a las redes o sistemas de la compañía.

- **Divulgación no autorizada de información personal.** Cuando se detecta una violación a la ley de datos personales, bien sea en relación con información bajo la tutela de la empresa o haciendo uso de su infraestructura tecnológica.

- **Acceso o intento de acceso sin autorización a un sistema informático.** Cuando se evidencia que personal no autorizado intentó acceder por el método que sea a los sistemas de la compañía o a sistemas de terceros pero haciendo uso de la infraestructura de la empresa.

- **Acceso o intento de acceso físico no autorizado.** Cuando una persona ingresa sin autorización a las áreas restringidas delimitadas por la empresa o cuando hay un intento de hacerlo.

- **Pérdida o destrucción no autorizada de información**. Cuando datos de valor para la empresa son eliminados, dañados o alterados de tal manera que no puedan ser legibles por sus propietarios sin la debida autorización.

- **Ingeniería social.** Cuando se evidencias intentos de atacantes internos o externos de obtener información relevante a través de engaños, entrevistas u otro tipo de seguimiento fraudulento dirigidos a los funcionarios de la empresa con el fin de obtener de ellos información privilegiada como claves

de acceso a sistemas, cuentas bancarias, buzones de correo u otro tipo de información que pueda ser aprovechada sin autorización. En este punto se registra la técnica tristemente célebre actualmente de phishing.

- **Interrupción en los servicios de comunicaciones.** Cuando a través de técnicas de denegación de servicio o por daño o alteración de alguno de los elementos de la infraestructura de comunicaciones de la empresa, los sistemas de comunicaciones son puestos fuera de servicio.

- **Uso indebido de correo electrónico institucional.** Cuando se evidencia que un funcionario está utilizando la cuenta de correo electrónico asignada por la empresa para cometer algún delito o para llevar a cabo actividades no autorizadas o explícitamente prohibidas por la empresa.

- **Anomalía o vulnerabilidad técnica del software.** Cuando se detecta que alguno de los activos de software de la empresa, sean de fabricación interna o externa, presenta un hueco de seguridad que puede o no haber sido aprovechado por un atacante.

- **Modificación de información de un sitio o página Web.** Cuando se evidencia que uno o más componentes pertenecientes a un sitio o aplicación Web de la empresa fue alterado sin autorización.

- **Robo o pérdida de equipo.** Cuando uno de los dispositivos tecnológicos de la compañía fue sustraído sin autorización o le fue robado al funcionario a quien le fue asignado, dentro o fuera de las instalaciones de la empresa.

- **Robo o pérdida de información.** Cuando una persona no autorizada, sustrajo información de la empresa o la modificó de manera que queda inutilizable o carente de valor.

- **Amenaza o acoso por medio electrónico.** Cuando a través de medios electrónicos que pueden o no ser propiedad de la empresa, se comete uno de los delitos mencionados.

- **Modificación, instalación o eliminación de software.** Cuando se evidencia que un elemento de software fue instalado, modificado o eliminado de uno de los sistemas de la compañía sin autorización.

- **Otro.** En este punto se deberá indicar cualquier actividad que haya provocado el incidente y que no corresponda a ninguno de los elementos ya mencionados.

- **Descripción del incidente.** Descripción no exhaustiva de las causas, efectos o cualquier otro dato relevante para una investigación que tenga que ver con el incidente reportado y su relación con los sistemas de la compañía.

- **Detección del incidente.** Descripción no exhaustiva de los indicios que llevaron a determinar la ocurrencia del incidente.

- **Duración del incidente.** Indicar en la casilla correspondiente si en el momento que se está realizando el registro del incidente, este aún persiste o si por el contrario se puede dar por terminado. En cualquier caso, indicar la duración del mismo en días, horas y minutos.

INFORMACIÓN SOBRE EL ACTIVO O BIEN AFECTADO

En esta sección se indican los datos de los activos de la empresa sobre los cuales el incidente tiene algún efecto o relación.

- **Descripción del activo o bien.** Indicar aquí el nombre del activo con el que el incidente está relacionado, preferiblemente tal y como aparece registrado en el inventario de activos de la compañía o en la matriz de riesgos vigente en el momento del registro. En caso de no tener a la mano esta información, se deberá describir el activo de tal manera que sea fácilmente identificable posteriormente.

- **Localización física.** Ubicación física donde se encuentra ubicado el activo, sea dentro o fuera de las instalaciones de la empresa, indicando si la ubicación es un lugar de acceso restringido.

- **Nombre y área del funcionario que tiene a cargo el recurso afectado.** Nombre completo del funcionario responsable por el activo que tiene relación con el incidente. Preferiblemente se deberá extraer esta información del inventario de activos de la compañía.

- **Copias de respaldo.** En caso de tratarse de activos de información, indicar en el campo correspondiente si existen o no copias del activo.

- **Ámbito.** En los campos correspondientes indicar si el activo afectado es responsabilidad directa de la organización. Se deberá marcar SI cuando el activo es propiedad de la empresa o cuando a nivel contractual esta asume la responsabilidad total o parcial de la administración del activo.

- **Conectividad.** Indicar en los campos correspondientes si el activo afectado tuvo en algún momento conexión a Internet. Se deberá marcar SI cuando en algún instante de tiempo el activo estuvo conectado, no necesariamente tuvo que estarlo en el momento de presentarse el incidente.

- **Sistema operativo.** En el caso en que el activo se trate de un equipo de cómputo, indicar bajo qué sistema operativo funciona.

Finalmente, cuando el formato ha sido diligenciado en un medio escribo, deberá ser firmado por el miembro del ERISI que realiza el reporte del incidente y de ser posible de deberá incluir la firma del funcionario que lo detectó e informó.

Elaborado por:	**Revisado por:**	**Aprobado por:**
GUILLERMO ÁLVAREZ Fecha: Noviembre de 2015		

Fuente: propio del autor.

ANEXO L. MANUAL DE FUNCIONES DEL EQUIPO DE RESPUESTA A INCIDENTES DE SEGURIDAD INFORMÁTICA

OBJETIVO

En este documento se describen las características del Equipo de Respuesta a Incidentes de Seguridad Informática de PTESA, en adelante denominado Grupo ERISI, comenzando por los antecedentes que llevan a su formación, los papeles que desempeña papel frente al cumplimiento de las políticas de seguridad de la información de la empresa, su estructura organizativa y las competencias personales y técnicas que deben tener sus miembros.

GLOSARIO

CERT. Siglas en inglés de Equipo de respuesta a Emergencias Informáticas (Computer Emergency Response Team). Es un grupo que está encargado de responder ante la ocurrencia de incidentes de seguridad en tecnologías de la información.

Ciberseguridad. Conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de una organización y los usuarios en el ciberentorno.

Competencias. Conocimientos, habilidades o destrezas que se adquieren y son necesarias para llevar a cabo adecuadamente una actividad en un ámbito determinado.

CCISO. Siglas en inglés de Oficial Certificado de Seguridad de la Información (Certified Chief Information Security Officer).

CISM. Siglas en inglés de Gerente Certificado de Seguridad de la Información (Certified Information Security Manager). Certificado con reconocimiento mundial de la persona que diseña, construye y gestiona programas de seguridad de la información empresarial.

CISSP. Siglas en inglés de Profesional Certificado de Sistemas de Información de Seguridad (Certified Information Systems Security Professional). Es una certificación con reconocimiento a nivel mundial que confirma el conocimiento de un individuo en arquitectura, diseño y gestión de controles que garantizan la seguridad de la información en entornos empresariales.

CONPES. Siglas de Consejo Nacional de Política Económica y Social. Es la máxima autoridad nacional de planeación en Colombia y se desempeña como organismo asesor del Gobierno en todos los aspectos relacionados con el desarrollo económico y social del país.

CSIRT. Siglas en inglés de Equipo de respuesta a incidentes de seguridad (Computer Security Incident Response Team). Este término se usa generalmente como un equivalente de CERT.

ERISI. Siglas de Equipo de Respuesta a Incidentes de Seguridad Informática. Se refiere al grupo de personas dentro de la empresa encargado de evaluar, documentar y gestionar los incidentes de seguridad informática.

Evidencia forense. Todo indicio que permite establecer a través del método científico, una relación entre un crimen y quien lo cometió.

HASH. Función matemática que a través de la aplicación de un algoritmo permite obtener un código de longitud fija a partir de unos elementos de entrada de datos.

Incidente de seguridad. Todo evento en el estado de un sistema que puede indicar una posible violación de la seguridad de la información, presencia de posibles fallas o cualquier hecho relevante para la seguridad.

Proxy. Término informático que se refiere a un equipo o servidor que hace intermediación entre un navegador Web e Internet permitiendo proteger y optimizar el acceso a la red.

Router. Dispositivo de red que permite el enrutamiento de paquetes de datos entre redes independientes de acuerdo a un conjunto de reglas definidas.

Switch. Dispositivo de red también conocido como conmutador o interruptor que permite la interconexión de equipos en una red.

Vulnerabilidad. Debilidad de un sistema informático que puede ser aprovechada por una amenaza para causar daños o alteraciones en un sistema informático.

ANTECEDENTES

A partir del año 2007 y en concordancia con el desarrollo e implementación del programa estatal Gobierno en Línea, se han adelantado en Colombia diversas iniciativas tendientes a establecer y consolidar grupos de respuesta a incidentes de seguridad de la información en las entidades del estado que estén articuladas con sus pares en el sector privado. De acuerdo con un estudio realizado por la división CERT del Instituto de Ingeniería de Software, entidad adscrita a la Universidad Carnegie Mellon, para Colombia “adoptar una

política nacional en ciberseguridad y ciberdefensa que involucre todos los sectores de la sociedad, bajo el liderazgo del Ministerio de Defensa Nacional en coordinación con otras entidades del estado, es un imperativo que debe tener la más alta prioridad".

Es así como en el año 2011 se emite un documento CONPES 3701 por el cual se establece la formación del colCERT, conformado por tres entidades de respuesta a incidentes a nivel nacional, como un primer paso para el fortalecimiento de la seguridad de la información en el país con el fin de afrontar las crecientes amenazas cibernéticas. Dos de los objetivos de estas entidades son:

Promover el desarrollo de capacidades locales/sectoriales así como la creación de CSIRTs sectoriales para la gestión operativa de los incidentes de ciberseguridad en la infraestructura crítica nacional, el sector privado y la sociedad civil.

Coordinar y asesorar a CSIRTs y entidades tanto del nivel público, privado y de la sociedad civil en la respuesta a incidentes informáticos.

Se evidencia así que la formación, mantenimiento y consolidación de equipos de respuesta a incidentes de seguridad de la información debe ser una prioridad para todas las organizaciones gubernamentales y del sector privado, particularmente aquellas que están relacionadas con la infraestructura crítica del Estado. Dado que el sector financiero hace parte de la mencionada infraestructura crítica y que PTESA se desenvuelve en ese ámbito, la conformación de un CSIRT es un tema que reviste suma importancia.

Políticas de Seguridad Informática de PTESA

Teniendo en cuenta las políticas de seguridad existentes en la compañía, se requiere incrementar la siguiente política relacionada con la administración de evidencia forense:

La atención y administración de incidentes de seguridad informática será realizada por personal interno que tengan conocimientos técnicos comprobables en la recolección y administración de evidencia forense.

FUNCIONES

El ERISI deberá desempeñar las siguientes funciones:

- Ser el canal formal de reporte de incidentes en la organización. Todos los funcionarios de la empresa deberán conocer a los miembros del equipo de tal manera que en el evento de la ocurrencia de un incidente, sepan dónde y a quién acudir.

- Asumir el rol de primer respondiente frente a los incidentes de seguridad informática.

- Documentar y gestionar casos a partir de los reportes de incidentes de seguridad. Una vez recibida la información de la ocurrencia de un evento, los miembros del ERISI serán quienes determinen si el evento es un incidente y así iniciar o no el procedimiento de gestión de incidentes.

- Analizar la evidencia recolectada. Si bien esta es una de las funciones del equipo, esta actividad no está contemplada en el procedimiento de captura y gestión de evidencia forense.

ESTRUCTURA ORGANIZACIONAL

De acuerdo a las políticas de PTESA, el máximo organismo que tiene competencia en asuntos de seguridad de la información es el Comité de Seguridad de la información, el cual es el encargado de coordinar y velar por el correcto funcionamiento de los esfuerzos de aseguramiento de los activos de información de la compañía. Por este motivo, el ERISI dependerá directamente de este órgano directivo que a su vez depende de la alta gerencia.

El ERISI estará compuesto por

- El Responsable de Seguridad Informática quien estará encargado de la selección, supervisión y capacitación del personal, asignación y distribución de presupuesto y ser el canal de comunicación formal con la alta gerencia.

- El Director del área de tecnología quien estará encargado de la administración y gestión de los recursos tecnológicos de la compañía, incluyendo aquellos que hayan sido asignados para la operación del grupo ERISI.

- Técnicos en seguridad informática. Como mínimo un funcionario con los conocimientos necesarios para realizar el levantamiento de evidencia forense de acuerdo con los lineamientos establecidos.

Dado que no es posible tener personal a tiempo completo dedicado a las labores de seguridad de la información, el responsable de seguridad informática será quien active el ERISI cuando ocurra un incidente de seguridad, involucrando a sus miembros conforme se presente la necesidad.

COMPETENCIAS

Con el fin de asegurar el adecuado accionar del grupo ERISI, todos los funcionarios que haga parte de él se deberán contar con las características personales que se describen a continuación

- Flexibilidad, creatividad y capacidad de trabajar en equipo.
- Alto nivel de análisis.
- Capacidad para trabajar de manera sistemática y ordenada.
- Honestidad y confiabilidad, saber administrar información confidencial.
- Capacidad para trabajar bajo presión y altos niveles de estrés.
- Buena capacidad para comunicarse de forma oral y escrita.

Los integrantes del grupo ERISI deberán además tener conocimientos técnicos acordes con el rol que van a desempeñar así:

- Conocimientos de la normatividad colombiana en relación con la seguridad de la información.
- Conocimientos en las amenazas de seguridad y de las técnicas de hacking más utilizadas.
- Conocimientos en equipos de infraestructura y tecnologías de red tales como routers, switches, proxy, etc.
- Conocimientos en administración de sistemas Windows y Linux.
- Conocimientos en técnicas de gestión de riesgos.
- Conocimientos en técnicas de identificación, recolección y gestión de evidencia forense tales como extracción de imágenes forenses, metodologías de cálculo y verificación de códigos HASH, técnicas de detección de vulnerabilidades entre otras.
- Conocimientos en técnicas de cadena de custodia.
- Experiencia mínima de 6 meses en la gestión de incidentes de seguridad.

Además de las mencionadas anteriormente, el Responsable de Seguridad Informática deberá contar con las siguientes características:

- Formación académica en seguridad de la información a nivel de Maestría y experiencia mínima de dos años en análisis y gestión de incidentes ó

- Certificación en una norma de gestión de seguridad de la información como puede ser CCISO, CISM o CISSP y un mínimo de experiencia de 4 años en análisis y gestión de incidentes de seguridad.

Elaborado por:	**Revisado por:**	**Aprobado por:**
GUILLERMO ALVAREZ Fecha: Noviembre de 2015		

Fuente: propio del autor.

ANEXO M. PROCEDIMIENTO PARA CAPTURA Y GESTIÓN DE EVIDENCIA FORENSE EN EQUIPOS DE CÓMPUTO DE LAS ÁREAS ADMINISTRATIVA Y DE DESARROLLO DE SOFTWARE DE PTESA

INTRODUCCIÓN

La evidencia forense es, por naturaleza, frágil y susceptible de alteraciones o modificaciones que pueden provocar la pérdida de valor probatorio. Para evitar que esto suceda se debe asegurar que las acciones adelantadas en relación con esa evidencia se ajusten a las normas y estándares internacionales de tal manera que pueda ser aceptada y utilizada eventualmente en posteriores procesos judiciales. Este procedimiento busca capturar de manera adecuada información forense que pueda ser de utilidad en un proceso legal o disciplinario manteniendo los principios de originalidad, integridad y admisibilidad de la evidencia.

GLOSARIO

Bitácora: Medio escrito donde se registran anotaciones que se consideran útiles para el seguimiento de una serie de eventos.

Cadena de custodia. Procedimiento de control que se aplica a elementos de evidencia desde su recolección hasta el final de su vida útil y que tiene como fin evitar alteraciones o cualquier contaminación o destrucción.

Datos volátiles: Datos que pueden contener evidencia forense que están almacenados en los medios de memoria volátil de un equipo de cómputo tal como la memoria RAM los cuales se pierden en el momento de interrumpirse el flujo eléctrico.

ERISI: Abreviatura de Equipo de Respuesta a Incidentes de Seguridad Informática. Se refiere al grupo de personas dentro de la empresa encargado de evaluar, documentar y gestionar los incidentes de seguridad informática.

Esterilización. Aplicado a medios digitales, es el proceso de eliminación segura de la información existente previamente en un medio de almacenamiento digital, es decir, sin que queden rastros de información que haya sido almacenada previamente en el medio.

Evidencia forense. Todo indicio que permite establecer a través de métodos científicos, una relación entre un crimen y quien lo cometió.

Imagen forense. Copia bit a bit de un medio de almacenamiento digital en la cual quedan grabados los datos tal y como se encuentran en el medio original.

Incidente de seguridad informática. Cualquier hecho que afecta o podría afectar la seguridad informática de la organización.

Interfaz de red. Dispositivo electrónico periférico que permite la comunicación en una red compartiendo recursos.

Medios de almacenamiento. Medios físicos donde es posible almacenar los datos de sistemas computarizados y posteriormente leerlos o recuperarlos.

Metadatos. Datos altamente estructurados que describen la estructura, contenido, calidad y condición de datos simples. Se conocen comúnmente como “datos acerca de los datos”.

Seguridad de la información. Conjunto de normas preventivas y reactivas que se toman frente a los sistemas de información de una organización con el fin de resguardar y proteger las características de la información: integridad, confidencialidad y disponibilidad.

Software. Término que se usa en informática para referirse a un conjunto de sentencias o rutinas que indican a un computador qué hacer.

ALCANCE

Este procedimiento se deberá ejecutar cuando existan reportes de incidentes de seguridad asociados con los equipos de cómputo que pertenecen a las áreas administrativas y de desarrollo de software de la compañía, incluyendo el área de pruebas utilizado para asegurar la calidad de los productos de software elaborados por la empresa. En este procedimiento no se incluyen los incidentes de seguridad relacionados con los activos de información existentes en el ambiente de producción. El procedimiento abarca las tareas de identificación, recolección, adquisición y preservación de elementos de evidencia digital.

DESCRIPCIÓN DE ACTIVIDADES

PLAN DE ACCIÓN

Durante la ejecución del procedimiento se deberá realizar las actividades que se enumeran y describen a continuación, cuyo desarrollo detallado se encuentra en la sección siguiente en este mismo documento. Las actividades se encuentran enumeradas siguiendo el orden secuencial en que se deben ejecutar, teniendo en cuenta que las actividades administrativas deberán ser ejecutadas en todos los casos, pero que la decisión de ejecutar o no cada una de las actividades restantes dependerá del nivel de criticidad asignado a cada incidente de seguridad, al tipo de activo de información involucrado, la naturaleza de la evidencia y la disposición de los elementos en la escena del incidente.

1. **Actividades administrativas.** Cubren labores de registro, clasificación y asignación de incidentes de seguridad. Describe las acciones que se deberán ejecutar una vez se reporta la existencia de cualquier incidente.
2. **Asegurar la escena del incidente.** Describen las primeras acciones que se llevan a cabo al iniciar un proceso de investigación a partir de un incidente con el fin de evitar pérdida o degradación de elementos de evidencia.
3. **Recolectar elementos de evidencia potencial no persistente.** Describe acciones que permiten recolectar elementos de evidencia que no se almacenan de forma persistente en los sistemas computarizados, comenzando desde los más volátiles a los menos volátiles.
4. **Recolectar dispositivos que contengan evidencia potencial persistente.** Describe las acciones que permiten recolectar o adquirir elementos de evidencia a partir de medios de almacenamiento de información digital.
5. **Asegurar y almacenar los elementos recolectados.** Describe las acciones de registro, protección y administración de los elementos de evidencia siguiendo los principios de cadena de custodia.

EJECUCIÓN

1. Actividades administrativas

En esta sección se cubren labores de registro, clasificación y asignación de incidentes de seguridad, las cuales se deberán ejecutar cada vez que se identifica un incidente de seguridad de la información en las áreas administrativas y de desarrollo de software de la compañía.

1.1 Reporte

Cuando se presenta un incidente de seguridad informática este debe ser reportado al grupo ERISI el cual realizará una valoración inicial, levantará un Reporte de Incidente de Seguridad en la bitácora y asignará al incidente un nivel de criticidad. Ver ***Instructivo para diligenciar la bitácora de incidentes de seguridad***. Si el nivel de criticidad es diferente de "Bajo", se iniciará un caso de investigación cuyo código de identificación estará formado por lo siguiente elementos separados por una raya baja (_):

- Número consecutivo que permite identificar el registro de la bitácora que da lugar al inicio del caso.
- Código de tres caracteres del área donde se presentó el incidente así: DES para el área de desarrollo y ADM para el área administrativa.
- Número consecutivo del caso.

1.2 Asignación

El Responsable de seguridad informática o un delegado suyo asignará a uno de los funcionarios activos del grupo ERISI -ver ***Grupo de respuesta a incidentes de seguridad informática*** - para que sea el encargado de procesar el caso iniciado por el reporte y se actualizará el registro del caso en la bitácora indicando el nombre del funcionario asignado.

Se deberán tener en cuenta los siguientes criterios para la asignación de casos:

a. Si el caso es catalogado como de nivel Alto, el Responsable de seguridad informática será quien personalmente asuma el caso y deberá contar con el apoyo de los dos miembros más experimentados del grupo ERISI.

b. Si el caso es catalogado como de nivel Medio o Medio Alto, será asignado como responsable el miembro del grupo ERISI con mayor experiencia que en el momento no esté asignado como responsable a un caso que aún esté abierto y contará con el apoyo de uno de los miembros con menor experiencia

c. Si el caso es catalogado como de nivel Bajo, será asignado a uno de los miembros del grupo ERISI que no cuentan con mucha experiencia con el fin de apoyar su proceso de aprendizaje.

2. Asegurar la escena del incidente

En esta sección se describen las primeras acciones que se llevan a cabo al iniciar un proceso de investigación a partir de un incidente con el fin de evitar pérdida o degradación de elementos de evidencia.

2.1 Preparación

Antes de iniciar las actividades técnicas propias de la intervención de la escena del incidente se deben realizar los siguientes preparativos:

a) Aprovisionarse de una libreta con hojas en limpio y lapicero para realizar anotaciones de cada una de las actividades a realizar.

b) Identificar el o los funcionarios responsables de los equipos de cómputo que se van a intervenir y la ubicación física de los mismos.

c) Revisar el inventario de hardware y software de la compañía para determinar los dispositivos instalados y la configuración asignada al equipo de cómputo que se va a intervenir.

d) Aprovisionarse de un medio de almacenamiento removible que esté esterilizado – ver ***Instructivo para esterilización de medios de almacenamiento*** - y que contenga espacio suficiente para tomar imágenes forenses de los medios de almacenamiento que tiene el equipo de cómputo que se va a intervenir.

e) Aprovisionarse de un medio de almacenamiento removible que contenga las herramientas de software apropiadas para la intervención. Ver ***Instructivo para recolección de datos volátiles***.

f) Aprovisionarse de una cámara fotográfica para realizar el registro documental fotográfico de la escena.

g) De manera opcional, cuando el incidente está catalogado como de Alta criticidad, se debería contar con un dispositivo de video para realizar el registro documental videográfico de la escena y del procedimiento.

h) De manera opcional, además de los funcionarios del grupo ERISI que hayan sido asignados, solicitar el acompañamiento, a título de testigo, de una persona que pueda dar fe de las acciones que se realizan, que puede ser el jefe del área donde se presenta el incidente o una persona con un cargo administrativo, según el tipo de incidente que da inicio al proceso de investigación.

2.2 Ejecución

Los pasos a realizar para asegurar la escena del incidente son los siguientes:

a) Tomar nota de la fecha y hora legal colombiana en que se dio inicio al procedimiento a partir de una fuente estandarizada que puede ser:

- La página Web dispuesta por el Instituto Nacional de Metrología de Colombia http://horalegal.inm.gov.co/.
- La línea telefónica nacional 117.

b) Anotar el número del caso de investigación forense asignado durante la fase de reporte del incidente y los nombres de los funcionarios que van a tomar parte en la ejecución del procedimiento y el rol que asumirá cada uno de ellos.

c) Desplazarse al lugar de la escena e identificar visualmente el equipo de cómputo que se va a intervenir y las personas que están presentes. Identificar y documentar cualquier situación anormal, como la presencia de dispositivos sospechosos, actividades anormales o inapropiadas de las personas presentes, o cualquier otro dato que se considere relevante para la investigación.

d) Verificar si entre los presentes en el lugar del incidente se encuentra personas ajenas a la compañía o personal no autorizado para estar en el área física donde se

presentan los hechos y tomar nota de sus nombres y de las razones que manifiesten al ser interrogados sobre su presencia en el lugar del incidente.

e) Tomar una foto panorámica del lugar donde se realiza el procedimiento en la que aparezca el equipo de cómputo objeto de intervención y de considerarse necesario, incluir la documentación fotográfica de las personas sospechosas. Verificar que las fotos no estén desenfocadas o faltas de nitidez.

f) Tomar fotos de los objetos circundantes y de los dispositivos conectados a los puertos e interfaces de red del equipo de cómputo. Verificar que las fotos no estén desenfocadas o faltas de nitidez.

g) Desconectar los dispositivos de red si existe alguno conectado. En caso de identificarse la presencia de dispositivos de red extraíbles conectados al equipo de cómputo objeto de investigación, ingresarlo en cadena de custodia. Ver ***Instructivo de cadena de custodia***.

3. Recolectar elementos de evidencia no persistente (volátiles).

En esta sección se describe acciones que permiten recolectar elementos de evidencia que no se almacenan de forma persistente en los sistemas computarizados, comenzando desde los más volátiles a los menos volátiles, las cuales se llevarán a cabo solamente si el equipo de cómputo objeto de intervención se encuentra encendido.

IMPORTANTE. Si el equipo de cómputo está apagado NO se debe encender.

a) Tomar fotos del contenido de la pantalla donde se pueda observar con claridad el contenido de cada una de las ventanas abiertas en caso de tratarse de equipos con sistema operativo Windows y de cada una de las ventanas, escritorios y consolas de comandos en uso en el caso de equipos con sistema operativo Linux. En este último caso, para verificar si se encuentran consolas de línea de comandos activas, se deberá usar la secuencia de teclas CTRL + ALT + [F1|F2|F3|F4|F5|F6].

b) Tomar nota de cualquier actividad anormal o sospechosa como en el caso de indicios evidentes de ejecución de software ilegal o malicioso.

c) Realizar recolección de datos volátiles –ver ***Instructivo para recolección de datos volátiles***.

4. Recolectar dispositivos que contengan evidencia

En esta sección se describen las acciones que permiten recolectar o adquirir elementos de evidencia a partir de medios de almacenamiento de información digital como se describe a continuación:

a) Si el equipo de cómputo está encendido, una vez se hayan recolectados los datos volátiles y los metadatos, se deberá apagar abruptamente el equipo de cómputo. Desconectar el equipo de la fuente de alimentación de energía eléctrica en el caso de los computadores personales que no cuentan con batería extraíble. Si el equipo cuenta con una batería, para forzar el apagado se deberá mantener oprimido el botón de encendido hasta que el equipo se apague abruptamente.

b) Realizar un inventario de los medios de almacenamiento para su posterior procesamiento -ver ***Instructivo para levantar inventario de medios de almacenamiento***.

c) Extraer imágenes lógicas de los medios de almacenamiento que pudieron verse afectados siguiendo el ***Instructivo para levantamiento de imágenes lógicas de medios de almacenamiento***.

5. Asegurar y almacenar los elementos recolectados

Todos los elementos de evidencia o de gestión documental recolectados o generados durante la ejecución del procedimiento, deberán ser puestos en cadena de custodia (ver ***Instructivo de cadena de custodia***) deberán por los miembros del grupo ERISI asignados al caso, y posteriormente deberán almacenarlos en un lugar con acceso restringido, protegidos en adecuadas condiciones físicas y bajo al menos un mecanismo de seguridad física como puede ser una gaveta bajo llave, la clave de una caja de seguridad u otro de la misma índole.

El presente documento y los documentos a los cuales se hace mención deberán ser administrados y actualizados periódicamente por el personal del grupo ERISI bajo la supervisión y tutela del Responsable de Seguridad de la información de PTESA y con la aprobación de la alta gerencia de la compañía.

Una vez se encuentre en ejecución, el Responsable de Seguridad de la Información deberá supervisar periódicamente el cumplimiento de cada una de las actividades descritas y asegurarse de que la documentación sea pertinente y que esté completa.

Elaborado por:	**Revisado por:**	**Aprobado por:**
GUILLERMO ÁLVAREZ Fecha: Noviembre de 2015		

Fuente: propio del autor.